OBLICI ŠTETE OD RAČUNALNIH VIRUSA I ODGOVORNOST ZA ŠTETU

Mr. sc. Katerina Dulčić, asistentica
Pravni fakultet Sveučilišta u Rijeci

UDK:
Ur.: 1. veljače 2007.
Pr.: 15. veljače 2007.
Izvorni znanstveni članak

Autorica u uvodnom dijelu rada opisuje oblike štetnih računalnih programa i štetne posljedice koji oni mogu izazvati. Potom iznosi slučajeve odgovornosti autora štetnih programa za štetu koju su izazvali i probleme u pogledu otkrivanja odgovorne osobe i utvrđivanja njene odgovornosti, te probleme utvrđivanja visine nastale štete te dužnosti oštećenika kako bi umanjio štetu i kako bi uopće spriječio nastanak štete. Pored toga, virusi i njima slični štetni programi mogu onemogućiti ili otežati ispunjenje obveza ugovornih strana iz ugovora o davanju usluga informacijskog društva. U radu su definirani ugovori informacijskog društva uz okvirno navođenje prava i obveza ugovornih strana, te koje posljedice mogu nastati ukoliko jedna od strana bude napadnuta virusom. Izložena su stajališta sudske prakse u Sjedinjenim Američkim Državama u takvim slučajevima i razlozi kojima se opravdavaju takvi stavovi, koji su doveli do usvajanja načela odgovornosti davatelja usluga informacijskog društva i u europskom zakonodavstvu.

Ključne riječi: *odgovornost za štetu, šteta, ugovor o uslugama informacijskog društva, ugovorna odgovornost, izvanugovorna odgovornost, računalni virus (malware).*

1. Uvod

Uz "invaziju" virusa koja opsjeda naša računala postavlja se pitanje koju štetu oni mogu izazvati i tko je za nju odgovoran. Računalo nam pruža olakšanje u radu, a danas je i internet postao usluga koju sve više osoba koristi. Koristeći se internetom izlažemo svoje računalo rizicima virusa, ali

to doživljavamo kao "nužno zlo", te smo prisiljeni stalno imati program koji nas štiti od virusa i redovito ga ažurirati kako bi nas štitio od novih virusa koji nastaju gotovo svakog dana.

Uvriježena je predrasuda da je oštećenik u slučaju kada šteta nastane zbog "zaraze" računalnim virusom ona osoba koja koristi računalo ili osoba koja je vlasnik računala, a čiji je korisnik zaposlenik. Međutim, kao što će kasnije biti izloženo u radu, oštećenik može biti davatelj usluga informacijskog društva (u svakodnevnom govoru: *provider*), ali i osoba koja uopće ne koristi računalo, ali čiji su osobni podaci pohranjeni na zaraženom računalu.

Isto tako se odgovornom osobom smatra osoba koja je izradila računalni virus, ali odgovorne za njegovo širenje mogu biti i neke druge osobe, o čemu će biti više rečeno u nastavku rada.

2. Što je računalni virus?

Računalni virusi zapravo su računalni programi kojima je osnovna funkcija proizvoditi neželjene učinke na računalu. Virus predstavlja program koji može inficirati druge programe, modificirajući ih tako da uključe kopiju njega samoga, koja također može biti modificirana. Pod infekcijom se smatra mogućnost virusa da ubaci svoje naredbe u postupak izvršenja programa, odnosno, pokušaj izvođenja legitimnog programa uzrokovat će i izvođenje virusa.[1] Ova definicija ključna je za određivanje virusa jer, potrebno je napomenuti, ne smatra se svaki maliciozni program virusom. Pogrešno je smatrati da je računalni program virus samo zbog toga što je destruktivan,[2] budući da postoje destruktivni programi koji su predviđeni računalnim sustavom i u okviru tog sustava imaju svoju korisnu namjenu (primjerice: naredba *Format*, koja se koristi za brisanje svih podataka s određenog medija).[3]

Prema svojoj strukturi virusi su računalni programi napravljeni kao i svi ostali programi koje korisnici koriste za rad na računalima, stoga računalo samo po sebi ne može uočiti razliku između programa kojeg korisnik želi na svom računalu i virusa. Efektivna razlika između virusa i "korisnih

[1] Ždranja, B.: Bestijarij u vlastitom domu, Bug, br. 134 (01/2004), str. 91.

[2] Vidi primjerice definiciju u Galašev, V.: Doktore, imam virus!, Enter, br. 9., 2003., str. 36.: "Svaki program kojemu je svrha da čini štetu na računalu spada u grupu tzv. zlonamjernih, štetnih, tj. *malware* programa (***Mal****icious Soft****ware***). Značajke ovakve vrste programa su oštećivanje, uništavanje i brisanje sustavskih ili korisničkih podataka te uzrokovanje nekontroliranih radnji i događaja na računalu ili cijelim računalnim sustavima." Iako to u samom tekstu nije naznačeno, potrebno je staviti naglasak na riječ "nekontroliranih", budući da destruktivne radnje, ukoliko su kontrolirane, u pravilu nisu štetne.

[3] Ždranja, B.: op. cit., str. 91.

programa" jest njihov rezultat: kod jednih željeni i koristan, a kod drugih neželjen i štetan.[4]

2.1. Vrste štetnih programa

2.1.1. Virusi u užem smislu

Iako su virusi uobičajeni "laički" naziv za sve štetne računalne programe, stručnjaci ih razvrstavaju u više različitih kategorija. Virusi (u informatičkom smislu riječi) su maleni računalni programi sa sposobnošću ubaciti se neprimjetno u druge računalne programe, postajući tako, naizgled, njegov sastavni dio. Automatski se sami umnožavaju, čineći različite oblike štete i neželjenih posljedica na zaraženom ili inficiranom računalu.[5]

Struktura virusa može se najlakše podijeliti u tri komponente, od kojih virus, prema svojoj definiciji, mora obavezno imati samo prvu. Prva komponenta predstavlja mogućnost infekcije. Ova komponenta specificira način na koji se virus širi. Kao što se vidi, nije nužno da virus radi ikakvu štetu na računalu, činjenica da se širi infekcijom dovoljna je da ga se okarakterizira kao virus.[6] Drugi dio virusa, koji nije obvezan, predstavlja nosivu komponentu (engl. *payload*). Ovaj dio definira sve aktivnosti virusa koje će biti izvedene uz njegovo širenje. Treći dio, koji također nije obvezan, predstavlja funkcija za okidanje (engl. *trigger*) koja definira vrijeme ili događaj prilikom kojeg će biti izvršena nosiva komponenta virusa.[7]

2.1.2. Računalni crvi

Računalni crv (engl. *worm*) je program koji neprestano umnožava sam sebe, zagušujući tako promet podataka na mreži ili zatrpavajući podacima tvrdi disk lokalnog računala sve dok se potpuno ne napuni. Za razliku od virusa, nema sposobnosti ubaciti se u drugi program i tako se dalje širiti. Programiran je na način da štetu čini u mrežnim sustavima pretvarajući se da izvršava dio poslova unutar mreže.[8] Osnovna razlika između crva i virusa je ta da crvi nemaju prvu i obveznu komponentu definicije virusa. Na adresu primatelja najčešće stižu u obliku privitka elektroničke pošte, ili koriste različite sigurnosne probleme, ali svima im je karakteristika da ne

[4] Correra, Michele M., Pierpaolo Martucci, Alessandro Ceresi: La fenomenologia dei "virus" nei computer crimes. Aspeti criminologici e giuridici, Rivista di polizia, br. IX., 1996., str. 551.

[5] Galašev, V.: op. cit., str. 36.

[6] Širenje infekcijom znači da se računalni program instalira na računalu i s njega na drugim računalima bez volje korisnika računala da instalira bilo koji program, dovoljno je samo pokretanje filea koji sadrži virus ili čak samo pristup određenoj "zaraženoj" Web-stranici (naravno ukoliko računalo nije zaštićeno antivirusnim programom).

[7] Ždranja, B.: op. cit. str. 91.

[8] Galašev, V.: op. cit., str. 36.

inficiraju druge programe.[9] Iako to ne znači da se crvi i virusi ne mogu "kombinirati" pa da tako crv koji se širi (i time remeti mrežni promet) može imati i komponentu koja instalira virus koji uništava podatke.

2.1.3. Trojanski konji

Trojanski konj (engl. *Trojan horse*), ili kraće trojan, program je koji se pretvara da izgleda kao i svaki drugi korisnički program, međutim, jednom kada se pokrene, otkriva svoje pravo lice i počinje izvršavati svoju (obično štetnu) zadaću, kao npr. formatiranje cijelog tvrdog diska. Za razliku od virusa i crva, trojanski konj se ne može sam umnožavati, već je za to potrebna aktivnost korisnika.[10] Pod trojanskim konjima obično smatramo programe koji na izgled rade nešto korisno i poželjno, a zapravo izvršavaju aktivnosti koje korisnik nije očekivao ili ne želi. Trojanski konji vrlo su često destruktivni ili pak pokušavaju "ukrasti" neke informacije s računala (npr. brojeve kreditnih kartica).[11]

2.1.4. Logičke bombe

Pored toga potrebno je razlikovati i logičke bombe koje su obično dijelovi trojanskog konja, ali se mogu nalaziti i u legitimnim programima. Postoji nekoliko potkategorija logičkih bombi, no njihova je zajednička karakteristika da predstavljaju funkciju ili skup funkcija koje se aktiviraju kada su ispunjeni određeni uvjeti. Najjednostavniji primjer logičke bombe je dio programa koji se aktivira npr. svakog prvog u mjesecu.[12]

2.2. Pojave slične virusima

Postoje i određene pojave[13] koje se po svojim učincima mogu svrstati u istu kategoriju s virusima. Tako, primjerice, povremeno se na internetu pojavljuju lažna upozorenja (engl. *Hoax*) u obliku najobičnije poruke elektroničke pošte, čiji je cilj masovno slanje i primanje kako bi se što više zagušio mrežni promet. Tim lažnim obavijestima dobronamjerno se upozorava na postojanje neke opasnosti (obično virusa) i traži se od korisnika da ju pošalje svim osobama čiju adresu ima na računalu. Na taj način korisnik sam obavlja funkciju virusa. Naime, korisnik primi poruku od osobe s kojom se uobičajeno dopisuje, koja može sadržavati i osobnu poruku pošiljatelja, a koja ga opominje na postojanje novog virusa kojeg ne prepoznaje niti jedan antivirusni program, a koji će se aktivirati

[9] Ždranja, B.: op. cit. str. 91.
[10] Vidi šire: Galašev, V.: op. cit., str. 36.
[11] Ždranja, B.: op. cit. str. 91.
[12] Ždranja, B.: op. cit. str. 93.
[13] U ovom slučaju ne možemo govoriti o računalnim programima, budući da to najčešće nisu, ali imaju slične štetne posljedice kao virusi.

u određenom kratkom roku i počiniti štetu na računalu. U slučaju da se u direktoriju Windows nalazi određena datoteka, potrebno ju je izbrisati. Svaki korisnik koji koristi Microsoft Windows, naći će tu datoteku, budući da se u tim lažnim obavijestima navede naziv datoteke koja jest sastavni dio operativnog sustava. Osoba koja povjeruje u takvu poruku, izbrisat će tu datoteku (posljedica čega će biti nestabilni rad računala ili njegova potpuna blokada), ali će i odaslati tu poruku svima koje poznaje, što će izazvati zagušenje prometa na mreži. Protiv ovakvih napada nema antivirusne zaštite, već jedino osposobljavanje i racionalni pristup korisnika.[14]

Spam, tj. neželjene komercijalne poruke, isto mogu izazvati štetu korisnika. Iako su one zabranjene Zakonom o telekomunikacijama,[15] svejedno se vrlo često pojavljuju.

Osim toga, iako djelatnost nije zabranjena, niti korisnici računala i interneta na nju gledaju jako negativno, slanje poruka elektroničke pošte koje sadrže zabavan sadržaj, ali koje su vrlo često "velike",[16] može izazvati smetnje u prometu računalnom mrežom vrlo slične virusima. Korisnik je najčešće želi poslati svim svojim znancima, i tako se dalje širi geometrijskom progresijom.

3. Pojavni oblici štete od virusa

Prva, iako najmanja, šteta koju će nam virus učiniti kada ga primimo putem interneta, jest neželjeni *download* podataka. Čak i u slučaju kada se naknadu za vezu s internetom ne obračunava ni po vremenu, ni po količini podataka koja se razmjenjuje, takva aktivnost usporit će rad računala, a time i rad osobe koja se njime koristi. Čak i ako antivirusni program otkrije virus i onesposobi njegov štetni učinak, ovaj dio štete uvijek postoji.

Postoje virusi koji su "bezazleni" prema korisniku računala, tj. nije im svrha učiniti štetu na podacima ili programima na računalu na koje stignu, već samo odaslati određenu poruku[17] ili ukazati na sigurnosne propuste programa koji se koristi za pristupanje internetskim stranicama (*browsera*) ili operativnog sustava.[18] Međutim, i takvi će virusi samom korisniku izazvati štetu u vidu gubitka vremena a, kao i svako neželjeno pokretanje

[14] Galašev, V.: op. cit., str. 37.

[15] Narodne novine, br. 122/03., čl. 111., te čl. 116. st. 1. t. 40., te slijedeći stavci istog članka.

[16] Sadrže privitke koji su ponekad i preko 1 MB veličine.

[17] Na primjer: crv W32/Cycle kojim je autor iznosio svoj stav o kvaliteti života u Iranu. <http://www.sophos.com/virusinfo/articles/cycle.html>

[18] Na primjer: 2003. godine pojavio se crv Blaster, a potom i crv Nachi (ili Welchi) koji je napravio veliku štetu a cilj mu je bio ukloniti crva Blaster i skinuti potrebne zakrpe s Microsoftova poslužitelja. Njegova "intencija" je bila dobra, ali je to rezultiralo zagušenjima računalne mreže.

nekog računalnog programa na računalu, vrlo često izaziva poremećaj u radu računalnog sustava.[19] Međutim, najveću će štetu izazvati pružatelju usluga informacijskog društva (*provideru*), odnosno onoj osobi koja pruža uslugu spajanja na internet. I takav će virus odaslati svoju kopiju na sve adrese koje se nalaze na računalu korisnika, naravno bez njegove namjere da to učini. Takav učinak izaziva zagušenje servera koji elaboriraju elektroničku poštu.

Kada autor virusa ima za cilj prouzročiti štetu na drugim korisničkim računalima, tada mogućnostima i idejama nema kraja. Moguće je čak i odabrati ciljnu skupinu, kao što je to, primjerice, i učinila "fantomska" kompanija iz Paname koja je još (u informatičkom smislu) daleke 1990. godine odaslala bolnicama, medicinskim institutima, ali i običnim privatnim osobama, disketu s računalnim programom koji utvrđuje mogući rizik izloženosti virusu HIV. Međutim, pored programa i podataka koji su bili vidljivi osobi koja je instalirala program na svoje računalo, disketa je sadržavala i virus koji se sam instalirao i aktivirao poslije nekoliko pokretanja računalnog sustava, a koji je pri tome onemogućio pristup podacima na tvrdom disku.[20]

Sami virusi mogu ili biti usmjereni na uništavanje ili mijenjanje podataka pohranjenih na računalu[21] ili na onesposobljavanje računalnih programa. Postoje, međutim, i virusi koji "napadaju" tzv. *boot*[22] sektor i koji izazivaju najveću štetu, jer je vrlo često nemoguće sanirati ju u smislu da pristup svim podacima i programima na tom tvrdom disku nije više moguć, pa je tada nemoguće i pokrenuti računalo.[23]

Pored toga potrebno je razmotriti i viruse poput crva *Sircam*,[24] čiji su autori primijenili pomalo perfidnu taktiku kako bi postigli da se čim više šire. Kako se ovaj virus širi putem elektroničke pošte, u poruku koju odašalje "krade" dijelove tekstova koje se nalaze na računalu s ciljem da bi onome tko primi poruku sadržaj bio primjeren pošiljatelju, te da s većom vjerojatnošću pokrene virus. Na taj način podaci koji mogu biti i povjerljivi dođu u vidu poruke elektroničke pošte do svih osoba čiju adresu elektroničke

[19] Correra, M. M., P. Martucci, A. Ceresi, op. cit., str. 553.

[20] Ibid., str. 554.

[21] Moguće je recimo ili da se datoteke brišu ili da se mijenjaju na način da se umjesto jednog znaka umeće drugi ili da se recimo kod brojčanih podataka zarez pomiče jednu znamenku lijevo ili desno.

[22] To je prvi sektor diska koji radi pod Disk Operating System (svi PC) koji sadrži program koji upravlja radom diska, koji kad se ošteti, više ne može omogućiti valjani rad tvrdog diska, odnosno memorije računala (ni programa na njemu, a niti omogućiti pristup podacima).

[23] Correra, M. M., P. Martucci, A. Ceresi, op. cit., str. 558.

[24] Vidi: Minotti, D.: Misure minime e operatori del diritto: tre pezzi facili - 1, Interlex, 15. 11. 2001., <http:www.interlex.it/_util/print.asp>; i < http://www.sophos.com/virusinfo/analyses/w32sircama.html>.

pošte na svom računalu ima osoba koja se zarazila virusom. Takav događaj može izazvati trećoj osobi imovinsku i/ili neimovinsku štetu.[25]

4. Pretpostavke odgovornosti za štetu od virusa

Da bi bilo koja osoba bila odgovorna za nastalu štetu, potrebno je utvrditi da postoje opće pretpostavke odgovornosti za nju, jer se u protivnom smatra slučajem.

Opće su pretpostavke odgovornosti za štetu da postoje subjekti odnosa odgovornosti za štetu, štetna radnja štetnika, šteta, uzročna veza između štetne radnje i štete te protupravnost. Pored toga se kod subjektivne odgovornosti zahtijeva i krivnja štetnika, a odgovara po objektivnoj odgovornosti (bez obzira na krivnju) samo kada je to zakonom propisano.[26]

Budući da je odgovornost za štetu od računalnih virusa nova pojava, potrebno je razmotriti gore navedene pretpostavke kako bi se jasno vidjelo koja osoba i u kojem slučaju odgovara za nastalu štetu i da li, uopće, netko odgovara za nastalu štetu ili se ona smatra slučajem ili pak višom silom.

Zakon o obveznim odnosima,[27] pored izvanugovorne odgovornosti za štetu, predviđa i odgovornost za štetu nastalu uslijed neispunjenja ugovora.[28] U slučaju informatičkih ugovora,[29] virus vrlo često može biti uzrok neispunjenja obveze, pa je potrebno razmotriti da li se radi o slučaju, višoj sili, odnosno, postoji li odgovornost za štetu zbog neispunjenja ili nepotpunog ispunjenja ugovora. Međutim, kao što će biti izloženo, virusi mogu onemogućiti i ispunjenje nekih drugih ugovora koji nisu u svojoj biti informatičke naravi.

[25] Vidi primjer spomenut u: Minotti, D., op. cit., koji opisuje slučaj odvjetnika kojem je računalo bilo zaraženo virusom Sircam i gdje je virus prilikom svog širenja preuzeo tekst iz jednog službenog dopisa koji je sadržavao sve osobne podatke o strankama (i stranci tog odvjetnika i protustranci) u jednom slučaju izvansudske nagodbe, koja je trebala biti povjerljiva. Treći, koji su primili te podatke nisu obvezni čuvati njihovu povjerljivost, pogotovo, ako bi ta objava bila od koristi njima ili njihovoj stranci.

[26] Klarić, P., Vedriš, M.: Građansko pravo, Zagreb, Narodne novine, 2006., str. 583. i slijedeće.

[27] Narodne novine, br. 35/2005., nadalje: ZOO.

[28] Čl. 9. ZOO.

[29] Sarazana di S. Ipolito, F.: I contratti di Internet e del commercio elettronico, Giuffrè, Milano, 2001., str. 59. i slijedeće.

5. Izvanugovorna odgovornost za štetu

Računalni virusi su od svog početka bili smatrani negativnom pojavom,[30] ali pravni problem bio je: kako kriminalizirati određena ponašanja, a da ista pravna regulativa ne remeti regularne aktivnosti na računalu.[31] Pravne norme koje reguliraju informatičku djelatnost moraju biti općenite s obzirom na to kako su učestale promjene u informatičkoj tehnologiji koje rezultiraju novim mogućnostima i novim aktivnostima. Stoga je u interesu država poticati razvoj i širenje novih tehnoloških rješenja, ali pri tome ipak nastoje suzbijati protupravne aktivnosti i naći normativnu ravnotežu koja je primjenjiva i u trenutku donošenja propisa, ali i još jedan duži vremenski period nakon toga.

5.1. Protupravnost izrade i širenja štetnih računalnih programa

Potrebno je razlikovati građanski delikt od kaznenog delikta. Osnova građanskog delikta je protupravnost štete ili neispunjenje obveze, dok se za opstojnost kaznenog delikta zahtijeva postojanje pravne norme koja određenu činjenicu predviđa kao kazneno djelo.[32]

Međutim, temeljem određenja kaznenog djela može se utvrditi protupravnost određenog djelovanja, te takvo protupravno djelovanje određenog subjekta čini pravnu osnovu izvanugovorne odgovornosti za nastalu štetu. Kazneno zakonodavstvo ne koristi izraz virus, što je i opravdano budući da su virusi samo uobičajeni naziv za računalne programe štetnog učinka, iako kao što je izloženo, i oni sami mogu biti vrlo različiti. Pravne norme pozivaju se na štetne učinke, odnosno posljedice djelovanja, bez obzira da li se radi o računalnom programu ili mehaničkom djelovanju.[33] Kažnjivi su pokušaji (bez obzira na njihov ishod[34]) onemogućavanja, otežavanja rada ili korištenja računalnih podataka ili programa, računalnih sustava ili računalnih komunikacija, odnosno neovlašteno mijenjanje tuđih podataka ili

[30] Što se da zaključiti i iz njihovog danas uobičajenog naziva, iako je to u početku bila metafora za *malware* – odnosno zloćudne računalne programe, pa se paralelno s time koriste i drugi izrazi vezani za medicinu kao inficirano računalo isl. Vidi šire: Klang, M.: A Critical Look at the Regulation of Computer Viruses, International Journal of Law and Information Technology, Vol. 11(2003.), No. 2, str. 163.

[31] *Ibid*.

[32] Franzoni, M.: L'illecito, Giuffrè Editore, Milano, 2004., str. 8.

[33] Članak 223. st. 2. i 3. Kaznenog zakona (Narodne novine, br. 110/97., 27/98., 129/00., 51/01., 105/04., nadalje: KZ) koji propisuje: "*Tko s ciljem onemogući ili oteža rad ili korištenje računalnih podataka ili programa, računalnog sustava ili računalnu komunikaciju, kaznit će se…"; "… tko neovlašteno ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivima ili nedostupnima tuđe računalne podatke ili programe."*

[34] Što znači da se može kazneno goniti i ona osoba koja je pokušala napraviti računalni program s određenim učincima, ali ga nije znala uspješno napraviti, slučajevi koji su u relativno kratkoj povijesti računalnog *malware*-a zabilježeni.

programa na računalu. Međutim, u slučaju samo (neuspjelog) pokušaja neće postojati građanskopravna odgovornost, zbog jednostavnog razloga što nije nastala šteta. Isto tako, prilikom zahtjeva za naknadu štete mora se dokazati konkretna šteta koja je nastala, za koju se ima pravo na naknadu.

5.2. Subjekti odgovornosti za štetu

Primjena pravnih pravila i načela građanske odgovornosti na internet primarno pati od problema individualizacije subjekta koji sudjeluju u protupravnim aktivnostima.[35] Primjerice, tako su u kolovozu 2003. godine veliku štetu na računalnim sustavima izazvali virusi *Blaster–A* i *Blaster–B*, te je autor virusa *Blaster–B* otkriven i nakon godinu i po' osuđen, a autor virusa koji je napravio još veću štetu, *Blaster-A*, još uvijek nije otkriven.[36]

Trojanske konje korisnici u pravilu sami instaliraju na svoje računalo u okviru nekog drugog programa, ali, u svakom slučaju, bez namjere instalirati štetan program, već onaj program koji skriva štetni program. U pravilu se radi o ponudi besplatnih programa koji mogu biti računalne igre ili čak programi koji se deklariraju kao zaštita od virusa. Ukoliko je štetan program takav da ne šteti računalu na koje je instaliran, već ga samo koristi kao bazu iz koje čini štetu ostalim računalima, korisnik, odnosno vlasnik, zaraženog računala nema saznanja, pa niti odgovornosti za štetu koju je počinio ostalim računalima. Tako se u Velikoj Britaniji vodio kazneni postupka protiv *Caffrey*ja (2003.), u kojem je oslobođen kaznene odgovornosti i temeljem utvrđenog činjeničnog stanja nije postojala niti pravna osnova za njegovu građanskopravnu odgovornost. Naime, *Caffrey* se u postupku branio tvrdeći da, iako je protupravna i štetna aktivnost polazila od njegova računala, on za to nije odgovoran, budući da je na njegovo računalo bio instaliran štetan računalni program kao trojanski konj, za kojeg on nije znao niti je morao znati. Utvrđeno je da s računala u vlasništvu gospodina *Caffrey*ja pokrenut napad s ciljem onemogućavanja usluga[37] prema računalnoj mreži Luke Houston koji je dosegao te razmjere da su određeni podaci potrebni za navigaciju bili nedostupni. Činjenica da li je računalo gospodina *Caffrey*ja bilo inicijator napada, nije bila sporna, ali je državni odvjetnik tvrdio kako se radilo o promašenom napadu na njegova prijatelja iz *chatroom*a, dok je obrana, naprotiv, tvrdila kako se radilo o napadu koji je posljedica trojanskog konja koji je zarazio to računalo. Prilikom vještačenja nije nađen

[35] Di Ciommo, F.: Responsabilità civili in Internet: i soggetti, i comportamenti illeciti, le tutele, <http://www.altalex.com/index.php?idstr=30&idnot=6878>, ulomak VII.

[36] <http://www.sophos.com/virusinfo/articles/parsonsentence.html>

[37] Napad s ciljem onemogućavanja usluga jest kada se na određenu računalnu mrežu istovremeno pokušava priključiti daleko veći broj korisnika nego što to ta mreža može podnijeti. To se može dogoditi slučajno, ali i tako da se na velik broj računala instalira *malware* koji bi automatski uspostavljao vezu s tim računalom i računalnom mrežom kojoj se želi onemogućiti ili otežati rad.

nikakav trag štetnog programa, ali je prihvaćena mogućnost da je štetan program postojao na tom računalu, a potom, sam sebe izbrisao nakon što je pokrenuo napad, iako je državni odvjetnik tvrdio da takva tehnologija ne postoji.[38] Ovakvi slučajevi ukazuju na problematiku dokazivanja za obje strane u postupku, te se računalo ponekad čini kao autonomno biće koje ima svoj život nad kojim njegov vlasnik ne može imati nadzor.

5.3. Krivnja štetnika

Autori virusa trebali bi odgovarati na temelju subjektivne odgovornosti, odnosno, trebalo bi utvrditi njihovu krivnju, budući da ne postoji pravna osnova za objektivnu odgovornost.[39] Zakon o obveznim odnosima propisuje kako se za stvari i djelatnosti od kojih potječe povećana opasnost štete za okolinu odgovara bez obzira na krivnju, te da se isto tako odgovara bez obzira na krivnju u slučajevima koji su predviđeni zakonom. Izrada računalnih programa može izgledati kao djelatnost od koje potječe povećana opasnost za okolinu ukoliko se radi o programu za računalo koje upravlja određenim strojem koji prema svojim karakteristikama jest opasna stvar, ali i tada možemo samo govoriti o opasnoj djelatnosti u smislu kako je uporaba tog stroja opasna i za koju postoji objektivna odgovornost, ali smatrati programiranje samo po sebi opasnom djelatnošću, nije prihvatljivo sukladno usvojenim pravnim stavovima.[40]

Stoga se autor virusa može osloboditi svoje odgovornosti ukoliko dokaže da je virus nastao pogreškom, odnosno ne njegovom namjerom, te da nije znao koje štetne posljedice može izazvati. Nezamisliva je situacija da autor virusa u užem smislu tvrdi da nije znao da je njegov računalni kod štetan, budući da ga upravo zato da bi se čim više proširio, bez obzira da li želi ukazati na propuste operativnog sustava, ili želi raširiti određenu poruku, ili jednostavno želi dokazati cijelom svijetu da je sposoban napraviti najinovativniji virus. Međutim, moguće je da je zaista netko ne dovoljno stručan ugradio neku logičku bombu u određeni računalni program, ne znajući točno što taj kod radi.

---

[38] Rowland, D., Macdonald, E.: Information Technology Law, Cavendish Publishing Limited, London, Sydney, Portland, Oregon, 2005., str. 451.–452. Autorice opisuju i slučajeve kada su osobe oslobođene optužbe zbog posjedovanja pedofilskih sadržaja tvrdeći da se radilo o trojanskom konju koji je bez njihova znanja na njihovo računalo prikupljano nedopušteni materijal.

[39] ZOO, čl. 1045. st. 3. i 4.

[40] "Neka je opasnost opasna djelatnost samo onda kada u njezinom redovitom tijeku, već po samoj njenoj tehničkoj prirodi i načinu obavljanja, može biti ugroženo zdravlje ljudi ili imovine, tako da to ugrožavanje zahtijeva povećanu pažnju osoba koje tu djelatnost obavljaju." VS, Rev-298/88., od 13. 10. 1988., PSP-43/76. Programiranje kao takvo u svom redovitom tijeku stvari ne ugrožava okolinu, već bi se to moglo eventualno dogoditi ukoliko se tim programom upravlja strojem koji je opasan po svojim drugim karakteristikama.

Zahtijeva se i svijest o štetnosti radnje koju se poduzima, što je bio razlog zbog kojeg je oslobođen odgovornosti devetnaestogodišnjak *Bedworth* u Velikoj Britaniji, koji je od svoje četrnaeste godine (kada je za rođendan dobio svoje prvo računalo) "provaljivao" u različite računalne sustave, te su se na listi njegovih žrtava našli *the Financial Times*, Institut za istraživanja karcinoma u Brusselesu, Uredi Europske zajednice u Luxemburgu i mnogi drugi, a koji su svi pretrpjeli znatnu imovinsku štetu. Iako je priznao da je navedene provale počinio, branio se tvrdeći kako je bio opsjednut, te su njegovi neovlašteni pristupi bili posljedica kompulzivnih radnji. Tako, iako je znao da čini protupravnu radnju, morao je nastaviti s daljnjim "provalama" budući da nije uspijevao nadvladati tu svoju protupravnu volju. Budući da se suđenje odvijalo pred porotom, ista ga je oslobodila odgovornosti. Iako se nikad ne može saznati zašto je porota donijela upravo takvu odluku, razvile su se razne teorije zbog čega je oslobođen. Prva jest: da su svojom odlukom članovi porote htjeli izraziti svoje neodobravanje britanskog Zakona o zloporabi računala (1990.), koji je predviđao vrlo stroge sankcije za počinitelje kaznenih djela koja su njime propisana, iako je to relativno malo vjerojatno. Druga je solucija da je porota ipak bila uvjerena kako se radi o određenoj vrsti ovisnosti, i to ovisnosti o računalima, što bi isključivalo njegovu ubrojivost u trenutku počinjenja djela, a isto tako postoji i mogućnost da je oslobođen zbog toga što su prema njemu primijenjene vrlo stroge mjere, a pogotovo s obzirom na činjenicu da se radilo o mladiću koji je svoju protuzakonitu aktivnost započeo s četrnaest godina, a uhićen je i optužen s devetnaest, te se smatralo da je policija pretjerala sa svojom reakcijom.[41]

5.4. Postojanje zahtjeva za naknadom štete

Tijekom 1999. godine mnoge računalne mreže bile su oštećene računalnim virusom nazvanim *Melissa*. Virus je napadao računala koja su koristila programe tvrtke Microsoft, šireći se na način da se sam poslao na prvih pedeset adresa upisanih u programu za obradu elektroničke pošte Outlook, te je ometao rad programa Word 97 i Word 2000. Virus je stizao kao važna poruka od prijatelja ili kolege, budući da je naizgled pošiljatelj bila osoba čije je računalo bilo zaraženo i nakon što bi ju primatelj otvorio, pokrenuo bi se virus koji bi automatski zarazio sljedećih pedeset računala. Prvi virus poslan je na listu koja je odašiljala poruke osobama koje su prihvatile primati vijesti u grupi "*Alt.sex*", a poruka je pozivala primatelje na otvaranje dokumenta u privitku napominjući kako sadrži ulazne kodove za internetske stranice sa sadržajem za odrasle. Stoga je inicijalno širenje koje je započelo 26. ožujka 1999. bilo vrlo brzo, što je izazvalo "zagušenje"

[41] Rowland, D., Macdonald, E.: op. cit., str. 447.–448.

servera koji procesuiraju elektroničku poštu. Visina štete koju je virus prouzročio procijenjena je na preko osamdeset milijuna američkih dolara, ali to je korišteno samo kao razlog visine kaznene osude, a štetnik *David L. Smith* nije bio obvezan naknaditi je, budući da se oštećenici nisu pojavili sa svojim zahtjevima za naknadu štete. Šteta se pojavila u vidu potrebe popravka računala te ometanja rada na računalima i računalnim mrežama korištenim u poslovne svrhe isto kao i vladinim računalima. Međutim, jedini cilj autora virusa bio je pokazati svoju sposobnost i uživati u pogledu na štetu koju je izazvao.[42] Razlozi zašto nisu postavljeni zahtjevi za naknadom štete mogu biti mnogi, ali u svakom slučaju potrebno je postojanje zahtjeva kako bi sud o njemu mogao odlučivati.

5.5. Uporaba virusa na "tržištu"

Vladalo je mišljenje kako je najveća štetnost računalnih virusa to što se šire velikom brzinom, a njihove su žrtve bili nasumice odabrani korisnici računala. Čak se nije moglo govoriti o korisnicima interneta, već upravo računala, budući da su se prvi virusi prenosili putem disketa i oštećenih računalnih programa. Virusi su pogađali u većoj mjeri velike informatičke strukture bile one javne ili privatne, ali i male korisnike osobnih računala u njihovim domovima.[43] Međutim, u novije vrijeme pojavljuju se ciljani napadi na određene računalne mreže ili korisnike, i to napose u pogledu onemogućavanja pristupa serveru, zbog čega je nemoguć i pristup pojedinim mrežnim stranicama. Budući da je internet prerastao svoje doba kada je isključivo bio namijenjen objavi informacija te se sve više koristi u tržišne svrhe, tako se može koristiti *malware* u svrhu suzbijanja konkurencije.

Unutar ilegalne sfere djelovanja razvili su se napadi koji se nazivaju "*denial of service*" ili DoS – napadi i "*distributed denial of service*" ili skraćeno DDoS – napadi, koji se sastoje u tome da se onemogućava pristup određenom serveru, a do toga dolazi zbog masovnog pristupa mnogih računala tom serveru.

Napadi za onemogućavanje usluga mogu se slikovito opisati kao "kada se u trgovinu pošalju stotine ljudi koji svojim upitima preopterete zaposlenike u trgovini te na taj način oni ne mogu opsluživati prave klijente. Vremenom nastane takva gužva u trgovini i ispred trgovine formira se dugi red u kojem

[42] <www.cybercrime.gov/melissaSent.htm>

[43] Correra, M.M., Martucci, P.: I nuovi svilupi dei reati informatici e la tutela della privacy, le banche dati nella professione medica, Studi in memoria di Maria Luisa Corbino, Facoltà di giurisprudenza della Università di Trieste, Milano, Giuffrè, 1999., str. 181. Autori koriste zanimljiv izraz kojim definiraju širenje virusa i na koji način su određeni potencijalni oštećenici: "*vittimizzazione 'a pioggia'*", budući da računalni virusi poput kiše pogađaju neselektivno sve koji i na najmanji mogući način mogu biti izloženi.

stoje "lažni" klijenti zajedno s pravim klijentima i na taj način je pravim klijentima uskraćen pristup usluzi."[44]

Napadi onemogućavanja usluge koriste karakteristike komuniciranja računala putem interneta, odnosno tzv. *Transfer Control Protocol / Internet Protocol* (uobičajeno: TCP/IP protokol), što je danas uobičajeni način komuniciranja računala putem interneta. Po tom protokolu komunikacija počinje kada računalo "klijent" zatraži uspostavljanje veze s računalom "serverom" šaljući mu tzv. "*SYN flag*". Server odgovara na način da otvara kanal za komunikaciju s tim računalom i čeka daljnju poruku s računala "klijenta". DoS – napadi vrše se putem jednog računala s kojeg se šalje velik broj "*SYN flag*"ova, bez namjere koristiti tako otvorene kanale za daljnju komunikaciju s računalom "serverom". Svaki server, pa kako se u praksi pokazalo i oni namijenjeni najvećem broju korisnika poput servera *Yahoo*, imaju ograničen broj mogućih kanala za komunikaciju, pa tako, ako je DoS – napad uspio, legitimni korisnici nemaju mogućnosti dobiti slobodan kanal za komunikaciju.[45]

Slična situacija se dogodila u Hrvatskoj kada je objavljena internetska stranica za pregled zemljišnih knjiga. Međutim, tu se nije radilo o ilegalnom napadu, već je zaista veliki broj drugih računala, odnosno, legitimnih klijenata, namjerno želio pristupiti tom serveru i pregledavati podatke objavljene na njemu. Došlo je do "zagušenja" mreže i njenih resursa, budući da se nije očekivao tako veliki broj korisnika koji će pristupati tom serveru u isto vrijeme. Ti su tehnički problemi riješeni povećanjem pristupne moći servera, ali i manjim brojem korisnika koji istovremeno pristupaju, budući da sada pristupaju samo oni korisnici koji su zainteresirani za podatke, a ne i velika količina znatiželjnika koji su to činili prvo vrijeme.

Kako bi se moglo razlikovati napade od legitimnih situacija povećanog interesa za određenu internet stranicu, osobe koje nadgledaju servere počele su voditi računa koliko "*SYN flag*"ova stiže prema njihovu serveru i da li oni stižu s istog računala ili različitih računala, te su na taj način počeli razotkrivati autore DoS – napada.[46] Kao logična posljedica toga pojavila se nova vrsta napada, tzv. distribuirano onemogućavanje usluge (DDoS), kada napad potječe s više računala istovremeno. Kako bi se moglo upravljati s više računala istovremeno, osobe koje su željele vršiti DDoS – napade počele su kreirati štetne programe (i to viruse, crve ili trojanske konje)

[44] Pinkney, K.R.: Putting the Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security – Related Software Failure, Albany Law Journal of Science & Technology, vol. 13. (2002.-2003.), br. 1. (2002.), str. 58.

[45] Pinkney, K.R., loc. cit.

[46] Tako je svojedobno i autoricu ovog članka kontaktirao (putem web-administratora Pravnog Fakulteta u Rijeci) web-administrator Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu budući da mu je bilo sumnjivo spajanje računala umreženog u sustavu Pravnog fakulteta na njihove internetske stranice, a prema IP adresi, odnosno broju koji čini adresu računala to nije bilo računalo informatičke službe.

koji im omogućuju upravljanje tuđim računalima, a prenose se bez znanja korisnika tih računala.[47]

Budući da su napadi onemogućavanja usluga usmjereni prema točno određenom računalnom sustavu, pojavila se mogućnost prodavanja takvih "usluga", odnosno prodaja sredstava za počinjenje takvih napada.

5.5.1. Šteta koja proizlazi od napada onemogućavanja usluga

Server koji se postavlja i putem kojeg se nude određene usluge ima predviđen broj korisnika koji se procjenjuje temeljem raznih parametara sličnih web–stranica koje već postoje na internetu, ali ukoliko se naglo poveća broj korisnika nekoliko puta, taj će server biti nedostupan. Sama činjenica da je određena mrežna stranica nedostupna, ruši ugled tvrtke koja svoje usluge prodaje ili samo reklamira na taj način. Pored toga to rezultira smanjenom, odnosno izgubljenom dobiti za razdoblje dok je usluga bila nedostupna i umanjenom dobiti za buduće razdoblje kada opet postane dostupna. Postoji tehnička mogućnost "zauzimanja" tuđih računala, ili čak svih računala na određenoj mreži koja se onda mogu "natjerati" u bilo koje doba da se bez znanja korisnika koji na tom računalu radi spajaju na određeni server, iako korisnik uopće nema taj interes i osoba se zasigurno svojevoljno i s opravdanim interesom ne bi spajala na određeni server svakih nekoliko minuta ili čak sekundi. Pored izgubljene dobiti za tvrtke čije se internetske stranice nalaze na istom napadnutom serveru, tu je i šteta koju pretrpe druge osobe u vidu troška popravka i osposobljavanja zaraženih računala i rada informatičara koji moraju računala "očistiti" od štetnih programa koji njima u radu, u pravilu, ne smetaju, ali izazivaju štetu drugima.

Pravo na naknadu štete imaju i oni prema kojima su usmjereni napadi i oni čiji se računalni sustavi koriste.[48] Odgovornima za štetu smatraju se ne samo autori štetnih računalnih programa nego i naručitelji napada, pa je tako u slučaju *U.S. v. Arabo* vođen kazneni postupak protiv naručitelja napada na internetske stranice svojih konkurenata, koji je tu uslugu naknadio počinitelju slanjem dizajnerske sportske odjeće prodajom koje se bavio. Obvezan je naknaditi štetu za izgubljenu dobit svojim konkurentima, iako sam nije poduzeo štetne radnje, ali je autoru virusa, koji se hvalio kako je sposoban to učiniti, obećao nagradu ukoliko učini nedostupnima internetske stranice njegova konkurenta. Unatoč tome što sam nije učinio ništa, niti je bio sposoban to učiniti, svejedno je obvezan naknaditi štetu koju su pretrpjeli njegovi konkurenti.[49]

---

[47] Detaljnije opise i tehnologiju DoS i DDoS napada vidi: Pinkney, K.R., op. cit. str. 57.-60.

[48] Vidi odluke američkog sudstva: U.S. v. Arabo, (D.N.J.), 25. kolovoza 2006., <http://www.cybercrime.gov/araboSent.htm>, U.S. v. Maxwell, (W.D.Wash.), 4. svibnja 2006., <http://www.cybercrime.gov/maxwellPlea.htm> i U.S. v. Ancheta (C.D.Cal.), 23. siječnja 2006., <http://www.cybercrime.gov/anchetaSent.htm>.

[49] U.S. v. Arabo, (D.N.J.), 25. kolovoza 2006., <http://www.cybercrime.gov/araboSent.htm>

Vlasnici računala s kojih polaze napadi ne smatraju se odgovornima, iako bi zapravo bili dužni primijetiti povećani promet koji polazi s njihove računalne mreže, međutim, u pravilu se smatraju žrtvama. Budući da autori ovakvih napada to čine, u novije vrijeme, radi ostvarivanja imovinske koristi, oni nastoje raširiti štetni program, putem njega imati pod svojom kontrolom velik broj računala, te potom čekati ne bi li našli klijenta koji bi platio određenu naknadu za usmjeravanje napada na određeni server, uz mogućnost da sami upravljaju tim napadom ili da to čini sam autor virusa.[50]

Tehnika ovladavanja računalima može biti vrlo sofisticirana, od jednostavnih trojanskih konja koji su ubačeni u naizgled bezazlene datoteke koje vlasnici računala sami preuzmu na svoja računala, kao što se primjerice u slučaju *Arabo* radilo o glazbenim datotekama u formatu mp3, ali može se raditi i o kompleksnom napadu kao u slučaju crva *Vierika*, kada je odaslana poruka elektroničke pošte koja je sadržavala datoteku pod nazivom "Vierika.JPG.vbs", koja ima dvostruku ekstenziju. Prva s oznakom JPG jest uobičajena oznaka za slikovne datoteke, pa su primatelji poruke, misleći da će pogledati sliku, otvorili datoteku koja je zapravo pokretala računalni program koji je smanjivao razinu sigurnosti Internet Explorera na najnižu razinu, te mu mijenjala početnu stranicu stavljajući onu stranicu na kojoj se nalazio štetni program. Taj se program, zbog niske razine zaštite na programu za pregled internetskih stranica sam, automatski, instalirao prilikom prve sljedeće namjere pristupanja internetu, budući da je već u Internet Exploreru kao početna stranica bila upravo ta, i na taj način otvarao mogućnost autoru virusa koristiti se tim računalom u trenutku kada mu to bude bilo potrebno.[51] Umanjenje sigurnosti računalnih sustava i ubrzano širenje otkriveno je na vrijeme, prije nego su zaražena računala upotrijebljena za napad na neki server. U ovom slučaju možemo govoriti samo o kaznenoj odgovornosti, a građanskopravna odgovornost bi bila upitna i teško bi ju bilo dokazati, jer još uvijek samim širenjem koda nije nužno nastala šteta vlasnicima računala. Posljedica štetne radnje autora virusa za korisnike računala bila je ta što im je bez njihova znanja smanjena razina sigurnosne zaštite računala, što je povećalo mogućnost zaraze drugim štetnim programima, a koji su mogli

[50] Vidi: U.S. v. Ancheta (C.D.Cal.), 23. siječnja 2006., <http://www.cybercrime.gov/anchetaSent.htm> U ovom slučaju autoru malicioznog koda oduzeto je više od 60.000,00 USD u gotovini i automobil marke BMW. On je prodro u računalnu mrežu Ministarstva obrane SAD-a i putem tih računala tražio ranjive računalne mreže te je tako kontrolirao s preko 400.000 računala u koja je ugradio maliciozni kod i potom je "ustupao" ta računala uz naknadu zainteresiranim klijentima. Nudio im je i izobrazbu kako se koristiti tim računalima i ustupao *software* koji im je bio potreban. Vjerojatno nije slučajno zašto je upravo za inicijalno računalo s kojeg je birao računala odabrao računalni sustav Ministarstva obrane, budući da je upravo ono koje i inače nadzire promet internetom, te stoga nije bilo sumnjivo kontroliranje drugih računalnih mreža koje je polazilo upravo s te računalne mreže.

[51] Vidi: Sentenza di Tribunale di Bologna, Proc. n. 11577/01 R.G.N.R., od 21. srpnja 2005. <http://www.penale.it/page.asp?mode=1&IDPag=182>.

izazvati štetu u vidu oštećenja ili gubitaka programa ili podataka. Međutim, u tom slučaju postavlja se pitanje je li korisnik primijenio svu dužnu pažnju kako bi izbjegao nastanak štete.

Tako, pored ranijih razloga zbog kojih se netko bavio izradom virusa i drugih štetnih programa, kao što su otuđenost, frustracija, želja za protagonizmom,[52] javlja se i nova pobuda, a to je laka i brza zarada, iako ilegalna.

5.6. Dužnosti oštećenika

U pravilu, štetu koju može počiniti neki virus zamišljamo kao oštećene ili izgubljene podatke ili eventualno nemogućnost uporabe određenog računala, no moguće su i puno pogubnije štete. Tako je primjerice prilikom pokušaja napada kojem je bio cilj ovladati računalnim sustavom jedne bolnice u Sjedinjenim Američkim Državama došlo do preopterećenja sustava koji je usporio rad te su nastali problemi u radu bipera liječnika, pristupa medicinskim kartonima pacijenata, ali i nemogućnosti otvaranja vrata operacijskih sala i gašenja računala na intenzivnoj njezi.[53] Štetnik je obvezan naknaditi štetu bolnici za sanaciju računalnog sustava, kao i Ministarstvu obrane. Pravo na naknadu štete bolnice opravdava se upravo time da su na vrijeme zamijetili napad, te su uspjeli spriječiti napad i pružati valjanu njegu pacijentima, a upravo njihova informatička služba obavijestila je FBI za vrijeme trajanja napada, pa je time i omogućeno otkrivanje počinitelja.[54] Bolnice ne bi smjele imati lagan pristup svom računalnom sustavu. U ovom slučaju radilo se o napadu kojem je cilj bilo samo instalacija programa koji će se koristiti za DDoS – napad, ali u drugom slučaju je bolničkim medicinskim podacima pristupila osoba osuđena za seksualne delikte i prikupila podatke o svojim potencijalnim žrtvama, te uputila opscene telefonske pozive četrnaestogodišnjakinjama.[55]

Međutim, svaki potencijalni oštećnik treba poduzeti sve potrebne mjere zaštite, jer osnovna je svrha interneta povezivanje udaljenih računala i virtualno smanjivanje udaljenosti, pa tako štetnice mogu biti na sasvim drugom kraju svijeta, što iz praktičnih razloga otežava mogućnost naknađivanja štete,[56] a ujedno je i vrlo upitno hoće li se ikada utvrditi tko je štetnik, s obzirom na anonimnost interneta.

---

[52] Vidi šire: Dragičević, D.: Kompjutorski kriminalitet i računalni sustavi, Informator, Zagreb, 1999., str. 148. i 149. i tamo citirana djela.

[53] U.S. v. Maxwell, (W.D.Wash.), 4. svibnja 2006., <http://www.cybercrime.gov/maxwellPlea.htm>

[54] Vidi: 2006 Westlaw 3158028 (W.D.Wash)

[55] Pierre, M.C.: New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy, Rutgers Law Review, vol. 56 (2003.-2004.), br. 2, str. 542.

[56] Franzoni, M., op. cit., str. 295.

Također korisnici interneta moraju biti svjesni da virusi postoje i da mogu počiniti štetu, te su dužni imati zaštitu od njih. Tako *Minotti*, u svom članku, napada korisnike računala koji su mu odaslali viruse starije od šest mjeseci, za koje postoje ažurirani antivirusni programi, a koji nisu bili svjesni da imaju zaraženo računalo. Posebno neodgovornima i u prekršaju smatra one koji na svojim računalima imaju osobne podatke drugih osoba, kao primjerice odvjetnik, ali svejedno naglašava kako bi svaki odgovorni korisnik računala u naše vrijeme morao imati na računalu programe koji sprječavaju i kontroliraju ima li na računalu neželjenih i štetnih programa.[57]

Slijedom toga, trebala bi se pretpostaviti mogućnost suodgovornosti oštećenika u nastanku štete, budući da nije poduzeo sve potrebne radnje kako bi spriječio nastanak štete ili ju umanjio.[58]

5.6.1. Utvrđivanje nastale štete i suodgovornost oštećenika

Izračun štete od virusa u pravilu je problematičan, jer još uvijek ne postoje ustaljene tarife radnog sata informatičara i nepouzdano je da li je utrošeni rad realan, ili je pretjeran, ali to su sporedna pitanja koja će praksa zasigurno riješiti. U svakom slučaju potrebno je vještačenje stručne osobe koja će točno utvrditi koja je šteta mogla biti spriječena i isto tako koja je šteta nastala uslijed neadekvatnog pokušaja saniranja štete. U drugom slučaju trebalo bi voditi računa o kojem se računalnom sustavu radi i da li su odgovorne osobe morale biti adekvatno osposobljene kako bi mogle procijeniti radi li se o mehaničkom kvaru na računalu, štetnom računalnom programu ili jednostavnoj grešci operatera koji je dao pogrešan nalog. Ova pitanja bila bi pojednostavljena kada bi i zakonodavac popratio određenom regulativom u pogledu obveze zapošljavanja stručnih osoba ili sklapanja ugovora o održavanju računalne mreže, barem za neke vitalne ustanove poput primjerice bolnica koje imaju računalnu opremu, ali ne nužno i stručnu osobu koja bi redovito održavala tu opremu. Ponekad naknada štete nije dovoljna kako bi naknadila izgubljeno, pa bez obzira što bi postojala odgovornost bolnica za tako nastalu štetu, bilo bi potrebno poduzeti mjere kako bi se spriječio nastanak štete.

Sudske prakse u vezi s naknadom izvanugovorne štete od računalnih virusa ima relativno malo s obzirom na količinu virusa i štetu koju izazivaju.

---

[57] Minotti, D.: Misure minime e operatori del diritto 1 i 2, 15. i 21. studenog 2001. godine, <http://WWW.interlex.it/675/minotti4.htm>; <http://WWW.interlex.it/675/minotti5.htm>

[58] Vidi čl. 1092. ZOO-a. Budući da ne postoji sudska praksa hrvatskih sudova možemo u svjetlu ove odredbe razmotriti slučaj bolnice napadnute hakerskim napadom u SAD-u. Unatoč svim sigurnosnim mjerama koje su proveli, ipak su pretrpjeli štetu, budući da je ta vrsta i oblik napada nepredvidljiv. Njihova se šteta sastojala u dodatnim radnim satima informatičke službe, te isto tako i drugog osoblja koje je imalo probleme u svakodnevnom radu. U istom slučaju odbijena je naknada štete jednoj školi koja je isto bila napadnuta od iste skupine hakera, ali nisu niti za vrijeme trajanja napada, a niti izvjesno vrijeme nakon toga, ustanovili da su bili napadnuti, što ukazuje na manjkavosti njihove informatičke službe.

Tvorce virusa i drugog *malware*a teško je identificirati, a onda, osim ako se ne radi o osobama koje su viruse radile radi prodaje na tržištu ilegalnih programa, te osobe nemaju dovoljno sredstava kako bi naknadile štetu koju su izazvale, a pored toga se vrlo često nalaze zemljopisno udaljeni od mjesta na kojem su izazvali štetu, što povećava troškove sudskog postupka.[59]

6. Ugovorna odgovornost za štetu od štetnih računalnih programa

Elektronička trgovina je provođenje trgovačkih aktivnosti i transakcija elektroničkim putem i obuhvaća različite aktivnosti, kao primjerice: nuđenje dobara i usluga elektroničkim putem, distribuciju putem računala (*on-line*) digitalnih sadržaja, izvršavanje burzovnih i financijskih transakcija putem interneta.[60] Iako ima autora koji elektroničku trgovinu definiraju isključivo kao aktivnosti koje nužno uključuju računalo, pored programskog rješenja i komunikacije,[61] međutim, u novije vrijeme javlja se i *Video on Demand*, kao specifičan oblik elektroničke komunikacije koji kao medij ne koristi računalo već televizijski prijemnik priključen na kablovsku ili digitalnu televiziju. Korištenje televizijskih prijemnika pokazalo se prihvatljivim i za smanjenje troškova pristupa internetu, pa se javljaju poslužitelji koji nude mogućnosti pristupa internetu na način da se televizijski prijemnik uz određene dodatke putem telefonskog voda (ili čak satelitske antene) spaja na internet.[62]

Hrvatski Zakon o elektroničkoj trgovini[63] ne sadrži definiciju elektroničke trgovine. Naime, ZET je donesen u okviru usklađivanja hrvatskog zakonodavstva s propisima Europske unije, te u cijelosti slijedi Direktivu 2000/31/EC, o određenim pravnim aspektima usluga informacijskog društva, a napose elektroničke trgovine, na unutarnjem tržištu ("Direktiva o elektroničkoj trgovini"). Sukladno članku 1. st. 1. ZET-a "*uređuje pružanje usluga informacijskog društva, odgovornost davatelja usluga informacijskog društva, te pravila u vezi sa sklapanjem ugovora u elektroničkom obliku*." Usluga informacijskog društva definirana je kao "*usluga koja se uz naknadu pruža elektroničkim putem na individualni zahtjev korisnika, a posebno Internet prodaja robe i usluga, nuđenje podataka na Internetu, reklamiranje putem Interneta, elektronički pretraživači, te mogućnost traženja podataka i usluga koje se prenose elektroničkom mrežom, posreduju u pristupu mreži*

[59] Lichtman, D.; Posner, E.P.: Holding Internet Service Providers Accountable, u: Grady, M.F.; Parisi, F.: The Law and Economics of Cybersecurity, Cambridge University Press, Cambridge, New York, 2006., str. 222.

[60] Delfini, F.: Il commercio elettronico, CEDAM, Padova, 2004., str. 4.

[61] Toplišek, J.: Elektronsko poslovanje, Založba Atlantis, Ljubljana, 1998., str. 3.

[62] Vidi šire: Gambino, A. M., L'accordo telematico, Giuffrè editore, Milano i Università di Roma Facoltà di giurisprudenza, Studi di diritto civile, 1997., str. 33.-37.

[63] Narodne novine, br.173/03., nadalje ZET.

ili pohranjuju podatke korisnika".[64] Iz navedene definicije vidljivo je da su usluge informacijskog društva pune širi pojam od kupoprodaje artikala putem interneta.

6.1. Ugovorne strane – davatelj usluga informacijskog društva i korisnik

Direktiva 2000/31/EC nosi podnaslov Direktiva o elektroničkoj trgovini, kojim se želi označiti njen sadržaj na sintetizirani način, odnosno uobičajeni naziv u kolokvijalnom govoru.[65] Time se htjelo naglasiti da sve ono što se uobičajeno naziva elektronička trgovina, zapravo su usluge informacijskog društva, te taj pojam obuhvaća elektroničku trgovinu, ali i mnoge druge usluge koje su neophodne kako bi se ona mogla ostvariti.

Direktiva 2000/31/EC definira davatelja usluga informacijskog društva kao bilo koju pravnu ili fizičku osobu koja pruža bilo koju uslugu informacijskog društva.[66] Hrvatski Zakon o elektroničkoj trgovini ne sadrži takvu odredbe, mada, logičkom dedukcijom, ista proizlazi iz samog zakona. Prema tome je pružatelj usluga informacijskog društva svatko[67] tko pruža usluge uz naplatu elektroničkim putem, sukladno čl. 2. st. 1. t. 1. ZET-a. Nakon toga su navedeni primjeri pravnih poslova koji se smatraju uslugama informacijskog društva, ali to su samo primjeri, a ne taksativno navedeni

---

[64] ZET, čl. 2. st. 1. t. 2. Ova definicija je zapravo preuzeta iz Direktive 98/48/EC, Europskog Parlamenta i Vijeća od 20. srpnja 1998. koja se odnosi na izmjenu Direktive 98/34/EC koja predviđa postupak informiranja na području normativa i tehničkih odredbi, a koja te usluge definira, ubacujući točku 2. u prvi stavak Direktive 98/34/EC, na slijedeći način:

"*2). "service": any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*

For the purposes of this definition:

" at a distance": means that the service is provided without the parties being simultaneously present,

" by electronic means": means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,

- "at the individual request of a recipient of services": means that the service is provided through the transmission of data on individual request."

Ovom odredbom definira se usluga, ali i "daljina" (koja za potrebe ove definicije označava činjenicu da ugovorne strane nisu istovremeno nazočne na istom mjestu), "elektronički put" (usluga odaslana na izvorištu i zaprimljena na odredištu putem elektroničkih uređaja za obradu, uključujući i digitalnu kompresiju, i memoriranje podataka i koja je u cijelosti prenesena, odaslana i zaprimljena putem žica, radio valova, optičkih sredstava ili drugih elektromagnetskih sredstava) i "individualni zahtjev primatelja usluge" (usluga koja je isporučena putem odašiljanja podataka na individualni zahtjev).

[65] Delfini, F.: op. cit. str. 3.

[66] Direktiva 2000/37/EC, čl. 2. st. 1. t. (b).

[67] I prema ZET-u to bi bila i fizička i pravna osoba, budući da se sam Zakon ne ograničava samo na pravne osobe, već sve osobe koje te usluge pružaju u okviru svojih djelatnosti.

svi pravni poslovi koje se takvima smatra. Zakonodavac je prisiljen koristiti vrlo okvirne definicije budući da se tehnologija mijenja velikom brzinom i cilj je propisa regulirati i sve buduće pravne odnose koji nastaju razvojem tehnologija, a ne trenutno zatečeno stanje. Direktiva 98/34/EC izmijenjena Direktivom 98/48/EC sadrži Aneks V kojim se pobliže objašnjava pojam usluga informacijskog društva na način da se isključuje primjena tehničkih standarda koje određuje ta Direktiva, ali na koju se poziva Direktiva 2000/31/EC kada se određuje njeno polje primjene. Tako se sukladno Aneksu V navode primjerice slučajevi kada se ne smatra kako se radi o pružanju usluge "na daljinu",[68] usluge za koje se smatra da nisu pružene putem "elektroničkih sredstava"[69] i usluge za koje se ne smatra da su "pružene na poseban zahtjev klijenta".[70]

U praksi ne postoje ugovori o pružanju usluga informacijskog društva, pod tim imenom, već se oni nazivaju s obzirom na konkretne usluge koje se pružaju tim ugovorom. Davatelj tih usluga se i u hrvatskoj tehničkoj terminologiji naziva engleskim nazivom *provider,* a širinu opsega njegovih djelatnosti možemo naslutiti kada sagledamo glavu "Odgovornost davatelja usluga informacijskog društva",[71] koja regulira slučajeve kada postoji izvanugovorna odgovornost davatelja usluga prema trećima, ali iz koje je vidljivo koje sve aktivnosti obuhvaća djelatnost davatelja usluga informacijskog društva, kao što je čisti prijenos podataka, privremena pohrana podataka i pohrana podataka.

[68] "Uslugama koje su pružene "na daljinu" ne smatraju se usluge koje su pružene uz fizičku nazočnost davatelja i primatelja usluge, iako uključuju uporabu elektroničkih naprava: a) liječničke pretrage ili liječenje u liječničkoj ordinaciji uz uporabu elektroničkih naprava, kada je pacijent fizički prisutan; b) pregledavanje elektroničkog kataloga u trgovini kada je klijent nazočan; c) rezervacija avionskih karti u putničkoj agenciji putem mreže ili računala, uz fizičku prisutnost klijenta; d) elektroničke igre koje su dostupne na primjerenom stroju kada je klijent fizički prisutan." Točka 1. Aneksa V.

[69] "Usluge koje nisu pružene "putem elektroničkih sredstava": I. Usluge koje imaju materijalni sadržaj iako su pružene putem elektroničkih naprava: a) automati za distribuciju gotovine ili karata (novčanice, željezničke karte); b) pristupanje cestovnim mrežama, parkirališta itd., naknada za korištenje, iako postoje elektroničke naprave na ulazima / izlazima koje nadziru pristup i / ili osiguravaju vršenje točne naplate. II. Usluge koje se pružaju off-line: distribucija CD medija ili računalnih programa na disketama. III. Usluge koje se ne pružaju putem elektroničkih naprava koje obrađuju / pohranjuju podatke: a) usluge telefonskih razgovora; b) usluge telefaksa i teleksa; c) usluge koje se pružaju putem telefonskih razgovora ili telefaksa; d) konzultacije liječnika puteme telefona ili telefaksa; e) konzultacije odvjetnika putem telefona ili telefaksa; f) direktni marketing putem telefona ili telefaksa." Točka 2. Aneksa V.

[70] "Usluge koje nisu "pružene na poseban zahtjev klijenta": Usluge pružene putem prijenosa podataka bez posebnog zahtijeva za simultani prijem neograničenog broja individualnih primatelja (prijenos s jedne točke na više točaka): a) emitiranje televizijskog programa (uključujući i usluge *near – video on – demand*), koje su obuhvaćene člankom 1. točkom (a) Direktive 89/552/EEC; b) usluge emitiranja radio programa; c) (televizijski) teletekst." Točka 3. Aneksa V.

[71] ZET, čl. 16. do čl. 20., Direktiva 2000/31/EC, Glava 4., čl. 12. do 15., iako se u Direktivi ispravnije ta glava naziva "Odgovornost posrednika".

Kako bi se utvrdile obveze davatelja usluga i korisnika, potrebno je sagledati ugovorene uvjete, bez obzira da li se radi o općim uvjetima koje je objavio davatelj usluga ili se radi o ugovornim odredbama koje su posebno pregovarane, budući da pravni propisi još uvijek ne sadrže odredbe kojima bi se regulirali u cijelosti odnosi koji nastaju prilikom pružanja usluga informacijskog društva.

6.2. Naplatni i besplatni ugovor u elektroničkoj trgovini

Iako definicija usluga informacijskog društva Direktive 98/48/EC predviđa pružanje tih usluga u okviru gospodarskih aktivnosti, odnosno, uz naknadu, njemački Zakon o teleuslugama[72] eksplicitno određuje kako se Zakon primjenjuje bez obzira da li je za uslugu predviđena naknada ili nije. Neki autori smatraju da to nije relevantno, budući da se u današnjem svijetu oni koji nude usluge nude putem interneta, to rade radi ostvarivanja profita, bez obzira da li se ostvaruje direktno od samih korisnika ili temeljem podatka o broju korisnika od sponzora. Iznimka su usluge koje pružaju vlada i njena tijela ili neprofitne organizacije.[73]

Zakonodavci su zauzeli stanovište da se osim u slučajevima koji su posebno regulirani propisima, na protupravnosti koje se dešavaju u virtualnom svijetu (*on-line*) primjenjuju normativni kriteriji koji reguliraju materijalnu realnost.[74] Stoga i kod elektroničke trgovine ugovorne strane moraju odgovarati za materijalne i pravne nedostatke ispunjenja svoje obveze. U teoriji i praksi usvojeno je stajalište kako u pravilu dužnik iz jednostranoobveznog odnosa ne treba odgovarati za nedostatke svog ispunjenja, budući da druga strana nema prema njemu nikakve obveze pa nema ni primjene načela jednake vrijednosti davanja, pa ni mogućnosti povrede tog načela.[75] Stoga je bitno razlikovati je li ugovor naplatan ili besplatan.

Činjenica da je njemački zakonodavac u Zakonu o teleuslugama naveo da se odredbe tog zakona primjenjuju na naplatne i besplatne usluge,[76] nije neosnovana, budući da kada se analiziraju pojedini ugovori o pružanju usluga putem interneta, vidi se kako je davatelj usluge predvidio za sebe ostvariti naknadu za tu uslugu koju pruža.

Ako se sagledaju ugovori o davanju pristupa internetu, a s obzirom na to da su *Internet Service Provider*i (ISP) uvijek (bar u dosadašnjoj praksi)

---

[72] Gesetz über die Nutzung von Telediensten, BGBl I 1997, 1870, I 2001, 3721., § 2. st. 3.

[73] Heyden, T.J.: Germany, u: Campell, D, ur.: E–Commerce and the Law of Digital Signatures, Oceana Publications, Dobbs Ferry (NY), 2005., str. 226.

[74] Di Como, F.: Evuluzione tecnologica e regole di responsabilità civile, Edizioni Scientifiche Italiane, Napoli, 2003., str. 166.

[75] Gorenc, V.: Komentar Zakona o obveznim odnosima, RRIF plus, Zagreb, 2005.(komentar uz čl. 357.), str. 529.

[76] Vidi *supra*.

pravne osobe koje se bave davanjem pristupa internetu kao jednom od svojih gospodarskih djelatnosti, iako ugovorom o pristupu internetu nije određena naknada u mjesečnom, godišnjem ili jednokratnom iznosu, po čemu je ugovor formalno besplatan, očito da je taj ugovor uvijek samo prividno besplatan.[77] U većini slučajeva naplata se vrši putem naplate prometa (bez obzira na to da li se isti računa putem količine prometa ili vremena trajanja veze), osim u slučajevima kada je održavanje sustava financijski potpomognuto iz trećih izvora, a radi ostvarivanja nekih drugih ciljeva (primjerice usluga pristupu internetu koju pruža CARNet, ustanova čiji je osnivač Vlada Republike Hrvatske, te mu stoga nije cilj ostvarivanje dobiti, već obrazovanja korisnika za korištenje računala, što uključuje i internet). Tako ako bi se pojavio spor u svezi s pruženom kvalitetom usluge, odnosno zbog njenih materijalnih nedostataka, ne bi se smjelo samo temeljem osnovnog ugovora koji ne predviđa plaćanje naknade od strane korisnika usluge isključiti odgovornost pružatelja usluge, već je potrebno sagledati širu sliku cjelokupne situacije i utvrditi da li se radi o ugovoru kojem je cilj ostvarivanje dobiti ili se radi o neprofitnoj organizaciji kao ISP-u.

Kod naplata usluge putem naplate prometa relativno je očito kako se radi o dvostrano obveznom ugovoru. Međutim, kod ugovora kao što je primjerice ugovor o adresi elektroničke pošte[78] *Googl*a (*Gmail*), naplatnost ugovora nije vidljiva na prvi pogled. Ako se opći uvjeti korištenja te usluge[79] pažljivo prouče, vidi se da u točki 7. tih uvjeta, pod nazivom Privatnost stoji: "*Činjenicom da se koristite Uslugom, prihvaćate odredbe Politike zaštite privatnosti* Gmail-*a, i to u smislu kako ona s vremena na vrijeme može biti mijenjana.* Google *shvaća da je privatnost vama važna. Ali, u svakom slučaju, vi pristajete da* Google *može nadzirati, mijenjati i otkrivati vaše osobne informacije, uključujući i sadržaj vaših poruke elektroničke pošte, ako bude to bude zatraženo radi ispunjenja obveze po valjanom pravnom sudskom ili upravnom nalogu (kao primjerice nalog za pretres, predaju isprava isl.),*[80] *ili u drugim slučajevima predviđenim ovim Općim uvjetima ili*

[77] Sarazana di S. Ipolito, F.: op. cit., str. 67.

[78] Kod ugovora o adresi elektroničke pošte zapravo se radi o ugovoru o najmu prostora na tvrdom disku računala. Sam prostor nije određen, budući da je davatelj usluge ovlašten, a ponekad može na to biti obvezan, prebacivati podatke na drugo računalo ili drugi tvrdi disk na istom računalu. Davatelj usluge je zapravo obvezan dati određenu količinu bitova na računalu koja mogu, ali i ne moraju, biti u njegovu vlasništvu. Obvezuje se da će unajmljeni virtualni prostor održavati u ispravnom stanju, a isto tako se obvezuje dati ispravnu programsku podršku koja omogućuje korištenje tog ugovorenog virtualnog prostora za primanje, čitanje i slanje elektroničke pošte. Vidi šire: Sarazana di S. Ipolito, F., op. cit., str.68.-76.

[79] Vidi Web stranicu: <http://mail.google.com/mail/help/terms_of_use.html>

[80] Ovo zadiranje u privatnost opravdano je i ako nije eksplicitno navedeno u općim uvjetima, svaki davatelj usluga informacijskog društva dužan je to učiniti i poštovati valjane sudske naloge. Iako ovlaštenje na mijenjanje može biti upitno, naime davatelj usluge mogao bi biti ovlašten spriječiti isporuku određene poruke, ako je ona po svom sadržaju ili namjeni protupravna, ali je niti tada ne bi smio brisati, već ju zadržati radi eventualnog kasnijeg dokaza,

Politikom zaštite privatnosti Gmaila. *Osobni podaci koje prikuplja* Google *mogu biti pohranjivani i obrađivani u Sjedinjenim Američkim Državama ili bilo kojoj drugoj državi u kojoj* Google Inc. *ili njegovi partneri imaju svoje pogone. Koristeći se* Gmail-*om, pristajete na svaki takav prijenos podataka izvan vaše zemlje.*"[81]

U točki osam Općih uvjeta, pod nazivom "Propagandne poruke" jasno je napisano što korisnik usluge daje kao naknadu davatelju usluge: "*Kao naknadu za uporabu Usluge, vi se slažete i razumijete kako će* Google *prikazivati oglase i druge podatke povezane i u odnosu na sadržaj vaših poruka elektroničke pošte.*"[82] Nadalje se objašnjava kako poruke elektroničke pošte neće čitati osobe, već se to čini putem računalnih programa koji će to automatski činiti, te neće pri tome mijenjati podatke u porukama elektroničke pošte. Isto tako *Google* se obvezuje kako neće adrese elektroničke pošte dati osobama čije propagandne poruke distribuira.[83]

Iako u Općim uvjetima usluge jasno stoji na koji način davatelj usluge prima naknadu za pruženu uslugu, koja čak omogućuje razmjernost međusobnih davanja: što se više koristi elektronička pošta, to se više podataka prikuplja i moguće je korisniku odaslati tim više komercijalnih promidžbenih poruka za koje davatelj usluga prima naknadu.

Iste ili slične oblike naplate koriste i ostali davatelji tzv. besplatnih usluga informacijskog društva. Tako i Politika zaštite privatnosti *Yahoo! mail*, u kojoj se nakon uvodne napomene o tome kako je davatelju usluga privatnost klijenata izričito važna, navodi kako *Yahoo!* prikuplja podatke i iz elektroničke pošte i na temelju internetskih stranica unutar *Yahoo!* i njegovih partnera, koje korisnik posjećuje te kreira profil korisnika, a ti

---

a mijenjanje sadržaja ne bi bilo nikada dopustivo, osim, naravno, ako korisnik na to ne pristaje, što u ovom slučaju čini.

[81] "*7. Privacy. As a condition to using the Service, you agree to the terms of the Gmail Privacy Policy as it may be updated from time to time. Google understands that privacy is important to you. You do, however, agree that Google may monitor, edit or disclose your personal information, including the content of your emails, if required to do so in order to comply with any valid legal process or governmental request (such as a search warrant, subpoena, statute, or court order), or as otherwise provided in these Terms of Use and the Gmail Privacy Policy. Personal information collected by Google may be stored and processed in the United States or any other country in which Google Inc. or its agents maintain facilities. By using Gmail, you consent to any such transfer of information outside of your country.*" <http://mail.google.com/mail/help/terms_of_use.html>

[82] <http://mail.google.com/mail/help/terms_of_use.html>

[83] "*8. Advertisements. As consideration for using the Service, you agree and understand that Google will display ads and other information adjacent to and related to the content of your email. Gmail serves relevant ads using a completely automated process that enables Google to effectively target dynamically changing content, such as email. No human will read the content of your email in order to target such advertisements or other information without your consent, and no email content or other personally identifiable information will be provided to advertisers as part of the Service.*", <http://mail.google.com/mail/help/terms_of_use.html>

podaci se koriste radi usmjeravanja propagandnih poruka, ali se prema trećim stranama poštuje anonimnost korisnika. [84]

6.3. Dužnosti ugovornih strana kod ugovora o pružanju usluga informacijskog društva

Dužnost korisnika usluga informacijskog društva jest pridržavanje pravila korištenja usluge, kao i prisilnih propisa koji zabranjuju određenu djelatnost i eventualno ugovoreno plaćanje novčane naknade. Ugovorne obveze davatelja usluge poduzimanje su svih mjera kako bi stalno mogle pružati ugovorenu uslugu korisniku.

Ne postoje tehnički standardi koji bi precizno određivali što je dužnost davatelja usluga kako bi se preventivno spriječio nastanak štete od virusa. Naime, ukoliko postoji objektivna nemogućnost ispunjenja ugovora, ugovor može biti ništetan[85] ili se zbog promijenjenih okolnosti može dužnik osloboditi svoje obveze ukoliko je činidba postala nemoguća zbog okolnosti za koje dužnik nije odgovoran. Na dužniku je teret dokaza da je činidba naknadno postala nemoguća bez njegove odgovornosti.[86]

U slučaju nemogućnosti ispunjenja činidbe zbog virusa potrebno je utvrditi da li je dužnik mogao predvidjeti i /ili spriječiti nastanak te štete, odnosno da li će se virus (odnosno bilo koji štetan računalni program – *malware*) tretirati kao slučaj ili viša sila.

Još uvijek ne postoje tehnički standardi za računalne djelatnosti kojima bi jasno bile propisane obveze svake osobe koja obavlja svoju djelatnost putem računala. Tako se u sudskoj praksi pojavljuje da se obveze dužnika određuju temeljem onoga što su njihovi konkurenti u to vrijeme činili.[87]

U slučaju *Cyber Promotions v. Apex Global Information Services*,[88] gdje je tvrtka *Apex Global* bila davatelj usluga pristupa internetu za tvrtku *Cyber Promotions*. U vrijeme sklapanja ugovora *Apex Global* je bila upoznata s činjenicom da se tvrtka *Cyber Promotions* bavi slanjem neželjenih promidžbenih poruka (tzv. "*spam*").[89] Temeljem ugovora o pružanju usluga pristupa internetu, *Apex* je imala pravo otkazati ugovor uz otkazni rok od 30 dana, ali kada je na *Apexov* server upućen masovni "*ping napad*" (što je oblik

[84] Vidi i Opće uvjete uporabe Yahoo!-a, <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html>, točke 3. i 4., <http://info.yahoo.com/privacy/us/yahoo/details.html>.

[85] ZOO, članak 270. st. 1.

[86] ZOO, članak 208. st. 1. i 2.

[87] Cook, W., Harrold, W.: Put Some Bite In Your Information Technology Protection, od It Can Bite You Back, Modern Practice Feature, January 2005, <http://practice.findlaw.com/feature-0105.html>, 23.1.2005.

[88] Cyber Promotions v. Apex Global Information Services, United States District Court, E.D. Pennsylvania, No. Civ. A. 97-5931. 30. rujna 1997., 1997. WL 634384 (E.D.Pa. 1997).

[89] I sam sudac se u svojoj odluci ogradio od razmatranja aktivnosti kojima se bavila tvrtka Cyber, iako je izrazio svoje neodobravanje takve gospodarske djelatnosti.

DDoS – napada) za koji su oni smatrali da je usmjeren na *Cyber Promotions*, kojem su odmah zbog toga prestali pružati uslugu bez poštivanja otkaznog roka od 30 dana za koje vrijeme bi *Cyber Promotions* imao mogućnost sklopiti ugovor s drugim davateljem usluga pristupa internetu i nesmetano nastaviti svoju djelatnost. Slijedom toga *Cyber Promotions* je podnio zahtjev sudu za privremenom mjerom kojom bi im se omogućio pristup ugovorenoj usluzi bez odgađanja uz zahtjev za naknadu štete. Sud je usvojio zahtjev, iako je *Apex* tvrdio da je "*ping napad*" bio izvan njegove razumne kontrole, za što se sukladno općim uvjetima mogao osloboditi odgovornosti, ali prilikom potpisivanja ugovora, *Apex* je bio upoznat s djelatnošću kojom se bavi *Cyber Promotions*, te da takva djelatnost može izazvati "*ping napad*" i izjavio je da će se moći nositi s takvom situacijom. Slijedom toga *Apex* je obvezan naknaditi izgubljenu dobit tužitelju i u najkraćem mogućem roku uspostaviti mu ponovno pružanje usluge pristupa internetu.

U siječnju 2003. godine tvrtka *Verizon* morala je platiti ugovornu kaznu Komisiji za javne usluge države Maine (*State of Maine, Public Utilities Commission*) budući da tijekom mjeseca siječnja nije pružala usluge na određenoj razini standarda. Ta je tvrtka imala ugovor o koncesiji za pružanje usluga pristupa internetu i audiotelefonije putem interneta za državu Maine. *Verizon* je tražio da im predviđena obveza bude umanjena budući da je pad razine usluga nastao zbog prilika koje su bile izvan njihove kontrole. Naime, njihov je sustav napao računalni crv *Slammer*,[90] te su bili prisiljeni isključiti svoje računalne sustave na oko dvadeset i četiri sata dok nisu našli sva napadnuta mjesta i sanirali kvarove izazvane računalnim crvom. *Verizon* nije mogao negirati postojanje ranijeg upozorenja proizvođača operativnog sustava u svezi s nedostatcima njihova proizvoda i pruženim mogućnostima kako bi se nedostatak sanirao na vrijeme prije napada. Komisija za javne usluge procijenila je kako je reakcija *Verizon*a nakon utvrđenog napada bila valjana i osnovano je računalni sustav isključen, budući da je u danim uvjetima to bila najbolja moguća obrana od širenja napada i saniranja štete, ali ipak su bili odgovorni budući da prije samog napada nisu bili adekvatno pripremljeni na njega. Argumente za ne usvajanje zahtjeva dale su konkurentske tvrtke *AT&T* i *WorldCom* koje su se u postupku protivile zahtjevu *Verizon*a. Ustvrdile su da je Microsoft programsku podršku za sanaciju tog nedostatka operativnog sustava stavio na raspolaganje 2. i 16. listopada 2002., više od tri mjeseca prije nego što se dogodio incident, te da argumentacija *Verizon*a kako je potrebno svaki novi računalni program prije

[90] Crv je napadao računala koja su koristila Microsoft SQL servere koji su radili na operativnom sustavu Windows 2000, ali je na taj oblik ranjivosti servera Microsoft upozorio još u srpnju 2002. godine (vidi upozorenje na službenim stranicama Microsofta: <http://www.microsoft.com/technet/security/alerts/ slammer.mspx>) te je dao i računalni program koji sanira tu ranjivost operativnog sustava. Crv nije činio štetu na podacima već je isključivo usporavao rad interneta prema napadnutim računalnim sustavima i iz tih računalnih sustava. Vidi šire: <http://www.sophos.com/security/analyses/w32sqlslama.html>.

instaliranja testirati, nije prikladna, budući da su oni uspjeli u tom vremenu instalirati i njihova računala nisu bili žrtve tog napada, te su nesmetano mogli nastaviti pružati uslugu svojim korisnicima sukladno propisanim standardima i ugovorenim uvjetima. Stoga je odlučeno da iako je napad crvom *Slammer* bio ozbiljan incident, to nije tako neočekivani i nepredvidljiv događaj koji bi bio obuhvaćen u standardima pružanja usluga kao razlog za ne plaćanje ugovorne kazne. U odluci nadležnog tijela naglašeno je: "Iako se ne pojavljuju učestalo, računalni virusi i crvi bili su nažalost sredstvo brojnih napada u prošlosti, a *Slammer* crv samo je posljednja verzija te vrste. Činjenica kako Microsoft više ili manje redovito izdaje obavijesti o sigurnosti, dokaz je se događaji ove vrste pre često događaju, te je potreban stalan nadzor."[91]

Teret dokaza kako su preventivne mjere zaštite bile adekvatne jest na dužniku, odnosno davatelju usluga koji nije pružio adekvatnu, odnosno ugovorenu razinu usluge. U slučaju nepružanja ugovorene brzine protoka podataka, postoji obveza naknade štete korisniku usluge.[92]

Donošenjem gore navedenih presudu u sustavu *common law* ne širi se ugovorna odgovornost, već se sužava definicija više sile i okolnosti koje su izvan mogućnosti kontrole ugovorne strane, davatelja usluga informacijskog društva.

6.3.1. Oslobađanje odgovornosti davatelja usluga informacijskog društva

U donošenju propisa koji su krajem prošlog stoljeća počeli regulirati djelatnost davatelja usluga informacijskog društva vladala je tendencija kojom se težilo oslobađanju odgovornosti davatelja usluga, kako bi se omogućio razvoj te nove djelatnosti. U Sjedinjenim Američkim Državama internet se počeo širiti dok je u Europi još bio u začecima, stoga su se i prvi pravni sporovi vezani uz internet pojavili pred njihovim sudovima koji su počeli postavljati određena načela. Postavljalo se pitanje da li na internet *provider*a gledati kao na osobu koja je pribavila sredstvo za počinjenje protupravne radnje,[93] čime bi bio suučesnik u protupravnom djelu ili će se

[91] State of Maine, Public Utilities Commission, Docket No. 2000-894, 30. travnja 2003., <http://www.maine.gov/mpuc/orders/2000/2000-849o.htm>.

[92] Vidi i odluku Mirovnog suda iz Bergama (Italija), Pedone c/ Video on Line s.r.l., od 15. ožujka 1996., <http://www.giuristi.thebrain.net/sententiae/civ/bergamo/index1.htm>, uvid: 10. veljače 1999.

[93] Tako je u presudi Playboy Enterprises, Inc. v. Frena iz 1993, 839 F. Supp. 1552 (M.D. Fla. 1993) provider oglašen odgovornim jer je omogućio sredstvo za širenje fotografija zaštićenih autorskim pravom, a u presudi Sega Entertainment, Ltd. v. Maphia iz 1994, 857 F. Supp. 679 (N.D. Cal. 1994) provider je također oglašen odgovornim jer je vodio internetsku stranicu na kojoj je dao programsku potporu distribuiranju računalih igrica koje su bile zaštićene autorskim pravom.

na njega gledati kao na osobu koja je samo dala "žice i cijevi" (*wire and conduits*).[94]

Odluka u slučaju *Religious Technology Center v. Netcom On–Line Communications Services* jest određena prekretnica, jer se počelo na davatelja usluge informacijskog društva gledati kao na osobu koja samo daje pristup materijalima na internetu, ali time nema dužnost vršiti nadzor, pa stoga, ukoliko u okviru svojih usluga ne nudi nadzor, ne postoji odgovornost davatelja usluge za objavljeni sadržaj. Time s pravnog gledišta nastaju dvije kategorije davatelja usluga informacijskog društva: oni koji samo daju pristup komunikacijskom kanalu i računalnoj mreži, slično kao telefonske kompanije, tzv. *access providers*, koji nisu odgovorni za sadržaj onoga što njihovi klijenti objavljuju na internetu putem njihovih servera, dok su, naprotiv, tzv. *service providers*, odnosno, oni koji osim pristupa internetu, pružaju svojim korisnicima i druge usluge (na primjer: računalne programe, grafičko sučelje i sl.), suodgovorni solidarno sa svojim klijentima za sav sadržaj koji je objavljen putem njihova servera. Posljedica je ove odluke da su pravni savjetnici tvrtki koje su se bavile pružanjem usluga informacijskog društva uputili svoje klijente kako je za njih sigurnije deklarirati se kao *access provider*, a ne kao *service provider*, i to na način da se javno putem samih internetskih stranica ograde od objavljenog sadržaja i da naglase slobodu njihovih korisnika na objavu sadržaja, suzdržavajući se od vršenja bilo kakvog nadzora ili kontrole. Analogija koja je primijenjena u odnosu na odnose ne-informatičkog svijeta bila je ona urednika i izdavača (*service provider*) i knjižare koja prodaje tiskovine i knjige (*access provider*), gdje je prvi odgovoran za sadržaj djela koja je izdao, dok drugi nije odgovoran za eventualne povrede prava trećih koja su počinjene putem sadržaja tiskovina ili knjiga koje prodaje u svojoj trgovini.[95]

Takav stav je zauzet i prilikom donošenja Direktive 2000/31/EC o elektroničkoj trgovini, koja regulira odgovornost davatelja usluga informatičkog društva prema trećima, oslobađajući ih odgovornosti u slučaju da ne mijenjaju sadržaj ili ne iniciraju slanje poruke. Naime, različiti stavovi u pogledu odgovornosti davatelja usluga informacijskog društva izraženi u propisima i sudskoj praksi zemalja članica Europske unije prije donošenja ove direktive sprječavali su razvoj ovih djelatnosti i pružanja ovih usluga bez obzira na državne granice. Cilj Direktive bio je i sprječavanje protuzakonitih aktivnosti koje se isto tako šire bez obzira na državne granice,

[94] Tako presudom Religious Technology Center v. Netcom On-Line Communication Services iz 1995, No. C-95-20091 RMW (N.D. Cal. Nov. 21, 1995) provider nije bio odgovoran zato što je na njegovim internetskim stranicama kojima je vodio news group-u objavljen tekst koji nije bio autoriziran, budući da nije pružao uslugu autorizacije niti nadzora sadržaja kojeg je unosio bilo koji korisnik. Stoga je sud zauzeo stav da osobu koja pruža takve usluge u virtualnom svijetu treba izjednačiti s onima koji u realnom svijetu pružaju usluge davanja žica i cijevi.

[95] Gattei, C.: Considerazioni sulla responsabilità dell'Internet provider, <http://www.interlex.it/regole/gattei2.htm>, 23. studenog 1998.

te je potrebno naložiti davateljima usluga da u takvim situacijama moraju djelovati. Direktiva je trebala postaviti ravnotežu između različitih interesa i uspostaviti načela na kojima se mogu temeljiti budući poslovni sporazumi i standardi.[96] Radi se o kompromisu između interesa davatelja usluga informacijskog društva koji su posrednici i koji ne smatraju kako bi morali, niti se smatraju u mogućnosti, vrednovati sadržaj informacija koje prenose ili obrađuju, napose s obzirom na dopuštenost i građanskopravnu štetnost prema trećima, i potrebu da se izbjegne mogućnost kako bi informatičke mreže bile u potpunosti izvan mogućnosti autoritativne kontrole.[97]

Oslobađanje odgovornosti davatelja usluga može imati negativne posljedice prema oštećenicima. Očit je primjer slučaj *Doe v. GTE Corporation i Genuinity Inc.*[98] *u kojem su u svlačionice i prostorije s tuševima sportskih sveučilišnih momčadi bile postavljene kamere, a na taj način snimljeni materijal kasnije je montiran i prodavan na način da je ponuda bila objavljena na internetskim stranicama koje su bile smještene na serverima tuženika, a distribuirale su se djelomično putem interneta, a djelomično putem pošte. Utužene su i tvrtke koje su prodavale te snimke, ali stoga što je nad nekima od njih okončan postupak likvidacije, a drugima nije bilo mogućnosti dostaviti tužbu jer se nisu znali njihovi podaci, postupak se vodio samo protiv dva davatelja usluga informatičkog društva. Sud ih nije smatrao odgovornima, budući da oni nisu izdavač ili govornik, i nisu ostvarivali oni profit prodaje videomaterijala pribavljenog bez suglasnosti subjekata koji su snimani. Iako ne bi bili sankcionirani u slučaju kada bi izbrisali takav materijal ili onemogućili pristup, nisu to bili dužni učiniti. Njihov je položaj uspoređen s položajem pošte i drugih dostavljača koji su dostavljali videokazete, a koji nisu bili niti utuženi.*

Slično kao i europska Direktiva 2000/31/EC i u Sjedinjenim Američkim Državama Zakon o pristojnosti informacija (Communications Decency Act, 1996.) određuje kako se davatelj usluga "interaktivnih računalnih usluga" ne može smatrati ni kao izdavač, ni kao govornik u pogledu informacija koje je pribavio drugi izvor sadržaja informacija. To u mnogočemu daje imunitet davateljima usluga u pogledu sadržaja koji su pribavili poslovni partneri ili sami korisnici, a u pogledu zaštite autorskih prava davatelj usluga nije odgovoran ukoliko djeluje samo kao prijenosnik materijala kojim se krše autorska prava. Odgovornost davatelja usluga je još manja ukoliko nije znao za protuzakonitu aktivnost, nije bio svjestan činjenica ili okolnosti u

[96] Vidi: Točke 40.-42 Preambule Direktive 2000/31/EC Europskog Parlamenta i Vijeća, od 8. lipnja 2000., o nekim pravnim aspektima usluga informacijskog društva, napose elektroničke trgovine, na Unutarnjem tržištu (Direktiva o elektroničkoj trgovini), Official Journal L 178, 17. 7. 2000. str. 0001-0016.

[97] Delfini, F.; op. cit., str. 177.

[98] John Doe and other memebers of football team at Illinois State University, at al. v. GTE corporation and Genuity Inc., United States Court of Appeals, Seventh Circuit, No. 02-4323, Oct. 21, 2003., WL 347 F.3d 655.

kojima se ta aktivnost odvija, nije ostvario neposrednu dobit od nedopuštene aktivnosti i ukoliko postupa po pravilima i tek po službenoj obavijesti spriječi pristup takvim materijalima pohranjenim na njegovim računalima.[99] S obzirom da su sudovi zauzeli tumačenje kako načela usvojena u propisu koji je donio Kongres SAD-a imaju veće značenje od onih usvojenim u propisima nekih država, to rezultira oslobađanjem odgovornosti davatelja usluga i u onim državama gdje bi po propisima te države bili odgovorni i obvezni skrbiti se o zaštiti svojih računalnih mreža.[100]

Upravo zbog činjenice kako se pri nuđenju drugih usluga, osim samog davanja na raspolaganje kanala komunikacije, odgovornost davatelja usluga proširuje i na sadržaj koji je objavljen, počele su se voditi rasprave u svezi s tim smije li davatelj usluge elektroničke pošte kontrolirati poštu kako bi se zaštitio od virusa. Naime, ukoliko bi davatelj usluga mijenjao poruke (na način da iz njih ukloni virus) ili spriječio njihovu isporuku (uz samo obavijest destinataru poruke o osobi koja mu je uputila poruku čija je isporuka spriječena zbog činjenice da je sadržavala virus), postojao je opravdani strah kako bi se netko mogao pojaviti sa zahtjevom za naknadu štete zbog toga što davatelj usluge nije spriječio isporuku poruke koja je sadržavala uvredu ili kojom je povrijeđen neki drugi propis, od autorskog prava do prava na privatnost, ili je putem poruka elektroničke pošte pripremano počinjenje nekog drugog kaznenog djela. Stoga su davatelji usluga informacijskog društva morali, prije nego su počeli pregledavati poruke elektroničke pošte antivirusnim računalnim programom, utvrditi kako oni ne zadiru u tekstualni sadržaj poruka, već samo provjeravaju da li poruka sadrži pored teksta i programsku komponentu koja se, po stručnom informatičkom mišljenju, sama pokreće, te kao takva čini virus. Činjenica jest da je u interesu davatelja usluga informacijskog društva ne imati korisnike čija su računala zaražena virusima, budući da takva računala povećavaju promet koji se može povećati do razmjera kada više davatelj usluge nije u mogućnosti svim svojim korisnicima pružiti ugovorenu razinu uslugu, a u tom slučaju postoji njegova odgovornost za neispunjenje ugovora, djelomično ili u cijelosti. S druge strane nemoguće bi bilo očekivati kako će davatelj usluga moći ostvariti naknadu štete od korisnika koji je zaražen virusom i koji je proširio virus svim ili većini korisnika čije adrese elektroničke pošte ima na svom računalu, a vrlo su često vezani na istog davatelja usluga, te je uslijed toga došlo do preopterećenja računalne mreže davatelja usluga. Naime, korisnik je vrlo često osoba bez informatičkog znanja i nije obvezna imati ga, kojoj se niti jednim propisom ne može nametnuti obveza instalacije antivirusnog programa na kućno računalo, te stoga ne može biti odgovorna ukoliko to računalo bude zaraženo virusom.[101]

[99] Digital Millennium Copyright Act, 17. U.S.C., § 512. a, c, d.
[100] Lichtman, D., Posner, E.P., op. cit., str. 222.-223.
[101] Što se može usporediti s obvezom postavljanja rešetki na prozore ili zatvaranja prozora

Danas, ipak, većina davatelja usluga informacijskog društva svojim korisnicima kontrolira poruke elektroničke pošte s ciljem sprečavanja širenja štetnih računalnih programa, bez obzira da li tu uslugu nude kao opciju koju korisnici mogu, ali ne moraju prihvatiti ili to čine za sve elektroničke poruke koje prolaze kroz njihov računalni sustav ne nudeći korisnicima mogućnost izbora. Taj postupak ne smatra se povredom privatnosti korisnika, budući da takav nadzor nije vezan za sadržaj poruke već za eventualno postojeću programsku komponentu poruke elektroničke pošte. Isto tako je usvojen stav kako se ta aktivnost ne smatra mijenjanjem poruke, pa stoga nema odgovornosti davatelja usluga informacijskog društva za sadržaj drugih poruka koje je propustio kroz svoj računalni sustav.

6.3.2. Tehničke mjere zaštite osobnih podataka

Iako tehnički standardi zaštite računalnih sustava nisu propisani posebnim propisima, niti se, u pravilu, preciziraju ugovorima, pojedine mjere zaštite propisane su u odredbama provedbenih propisa koje određuju tehničke standarde za zaštitu osobnih podataka. Pohranu osobnih podataka neki autori smatraju opasnom djelatnošću,[102] budući da je dobro koje se tim odredbama štiti osobno pravo svake fizičke osobe, a rizici su veliki i osoba čiji se osobni podaci čuvaju ne mora biti i najčešće nije upoznata s tim rizicima.

Europska Direktiva 95/46/EC Europskog parlamenta i Vijeća o zaštiti pojedinaca s obzirom na obradu osobnih podataka i slobodnom prometu takvih podataka (nadalje: Direktiva 95/46/EC)[103] svojim člankom 17. regulira obvezu država članica na donošenje propisa kojima voditelji zbirki osobnih podataka obvezuju štiti svoje baze podataka odgovarajućim tehničkim i organizacijskim mjerama. Time bi ih zaštitili od slučajnog ili protupravnog uništenja, slučajnog gubitka, izmjene podataka, neovlaštene objave ili pristupa podacima, a napose u slučajevima kada obrada podataka uključuje slanje osobnih podataka putem mreže, a isto tako dužni su zaštiti osobne podatke od svih protupravnih oblika obrade. Nadalje, Direktiva 95/46/EC određuje čime se potrebno voditi prilikom određivanja tehničkih standarda koje svaki voditelj zbirke osobnih podataka mora uspostaviti kako bi bio ovlašten prikupljati, obrađivati i čuvati osobne podatke drugih osoba. Tehnički standardi trebaju pratiti razvoj tehnologija, ali se prije nego se voditelji zbirki osobnih podataka mogu obvezati na njihovo uvođenje, mora razmotriti i cijena uvođenja tih novih tehnologija. Cilj je takvih mjera osigurati razinu sigurnosti primjerenu riziku koji predstavlja obrada

vlastitog stana, što je obveza onih koji su preuzeli obvezu čuvanja tuđih stvari, ali ukoliko osoba ne zaključa vlastiti stan, može izgubiti pravo na naknadu temeljem police osiguranja od krađe, ali to ne možemo smatrati obvezom.

[102] Franzoni, M., op. cit., str. 299. i str 357-363

[103] Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

podataka i vrsta podataka koju treba zaštititi. [104] Činjenica jest kako se ne može zahtijevati uspostava iste tehničke razine zaštite za prikupljanje osobnih podataka bolnicama ili lokalnom nogometnom klubu koji vodi evidenciju svojih članova.[105]

Direktiva Europske unije nije tip propisa koji bi mogao i trebao određivati tehničke standarde koje bi voditelji zbirke osobnih podataka trebali primijeniti kako bi se moglo reći da su ispunili svoju obvezu koja proizlazi iz zakona ili ugovora na čuvanje osobnih podataka. Naime, nepobitno jest kako napad štetnim računalnim programima može izbrisati, izmijeniti ili učiniti nedostupnima podatke koji su pohranjeni na računalu, pa samim time i osobne podatke vlasnika računala ili drugih osoba čije podatke vlasnik računala čuva. Novine u računalnoj tehnologiji gotovo da su svakodnevne, pa je s toga nemoguće pratiti ih i normirati putem propisa kao što je direktiva Europske unije, koja uvijek sadrži i određeni rok u kojem je moraju usvojiti države članice, pa stoga, zapravo, prema onima koje bi taj propis trebao štititi, stupa na snagu s dugom vakacijom, što bi u ovom slučaju značilo u trenutku kada je to s tehničkog aspekta već zastarjelo.

Njemački Savezni zakon o zaštiti osobnih podataka[106] u § 9. određuje samo kako su osobe koje obrađuju osobne podatke u svoje ime ili to čine za drugoga, dužne provoditi tehničke i organizacijske mjere zaštite sukladno načelima koja određena Aneksom Zakona. Njime su određena načela što treba biti zaštićeno s obzirom na različite faze obrade osobnih podataka, pa se tako zahtijeva da voditelj zbirke osobnih podataka uredi ovlaštenja pristupu osobnih podataka, prijenosu osobnih podataka, unosu podataka, a posebna je i odredba o tome na koji se način moraju obrađivati podaci ukoliko se obrada vrši za drugu osobu, osigurati trajnu dostupnost podataka kako ne bi bili slučajno uništeni ili izgubljeni, te zahtjev za odvojenom obradom podataka koji su prikupljeni u različite svrhe.[107] Iako takav pristup ne sadrži eksplicitno zahtjev za postavljanje antivirusne zaštite, ona proizlazi iz odredbe točke 2. Aneksa BDSG-a koja određuje kako treba onemogućiti neovlašten pristup podacima, odredbe točke 4. koja zahtijeva mjere osiguranja prilikom prijenosa podataka i najviše točke 7.

[104] Čl. 17. st. 1. Direktive 95/46/EC.

[105] Iako je Tijelo za zaštitu podataka Velike Britanije izrazilo zabrinutost budući da se prilikom davanja podataka na obradu drugim osobama u Velikoj Britaniji zahtijevaju isti standardi nadzora i za zbirke osobnih podataka ovako malog značenja i rizika. Vidi: Korff, D.: EC Study on Implemantation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49), Comparative Summary of National Laws, Human Rights Centre, University of Essex, Colchester (UK), Cambridge (UK), 2002., str. 159.

[106] Bundesdatenschutzgesetz, vom 20. Dezember 1990 (BGBl. I S. 2954), neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), geändert durch § 13 Abs. 1 des Gesetzes vom 5. September 2005 (BGBl. I S.2722) sowie durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970). Nadalje: BDSG

[107] Vidi aneks BDSG-a točke 1-8.

koja propisuje obvezu zaštite podataka od njihova slučajna uništenja ili neželjenih izmjena.

Pored toga njemačko Tijelo za zaštitu podataka i slobodu informacija (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) na svojim internetskim stranicama objavljuje kontinuirano stručne savjete u pogledu tehnološke orijentacije,[108] daje precizne tehničke savjete kako primijeniti aktualnu tehnologiju i koje mjere zaštite te upute što je potrebno učiniti kako bi se računalo zaštitilo od virusa. To zapravo čini Savezni ured za sigurnost informatičke opreme (*Bundesamt für Sicherheit in der Informationstechnik*), stručno državno tijelo koje se skrbi o sigurnosti informatičke tehnologije. Poštivanje tamo objavljenih preporuka ne može se smatrati obvezom voditelja zbirke osobnih podataka, ali budući da se radi o minimalnim standardima (jer se preporuča obnavljati podatke o novim virusima u antivirusnom programu najmanje jednom mjesečno, dok tvrtke koje proizvode i prodaju programe za zaštitu od virusa nove podatke o novim virusima nude gotovo svakodnevno, a ponekad i više puta dnevno), voditelj zbirke osobnih podataka koji nije poduzeo te minimalne mjere zaštite svakako bi bio odgovoran ukoliko dođe do štete zbog gubitka, oštećenja, izmjene ili neovlaštenog širenja podataka.

Talijanski Pravilnik o utvrđivanju minimalnih mjera sigurnosti za obradu osobnih podataka određuje kako sredstvo kojim se obrađuju podaci mora biti osigurano od računalnih programa koji imaju za cilj ili učinak oštećenje računalnih sustava, podataka ili programa koji su u njima sadržani ili im pripadaju ili potpuni ili djelomični prekid ili poremećaj njegovih funkcija.[109] Učinkovitost i ažurnost tih programa potrebno je, prema Pravilniku, kontrolirati semestralno.[110] Rok od šest mjeseci možda je bio adekvatan u vrijeme donošenja ovog propisa, 1999. godine, ali danas je potrebno imati gotovo dnevno ažuriranje, ako ne i češće, i isto tako stalno se informirati u pogledu novih štetnih programa koji se pojavljuju. Iako je propisom predviđena obveza tako rijetkog testiranja programa, ne bi se moglo smatrati savjesnim voditeljem zbirke osobnih podataka drugih osoba onu osobu koja nema osiguranu odgovarajuću zaštitu tuđih podataka primjerenim računalnim programima što se nude na tržištu i koji svoje podatke o štetnim programima koje treba sprječavati ne ažuriraju stalno dok je računalo spojeno na internet.

---

[108] <http://www.bfdi.bund.de/cln_029/nn_530436/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/TechnologischeOrientierungshilfen__node.html__nnn=true>

[109] Definicija na koju se poziva Pravilnik sadržana je u talijanskom Kaznenom zakoniku, čl. 615. quinquies.

[110] Čl. 4. st. 1. točka c), Decreto del Presidente della Repubblica n. 318 del 28 luglio 1999., Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996.

Temeljem Zakona o zaštiti osobnih podataka,[111] Vlada Republike Hrvatske donijela je Uredbu o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka.[112] Njom se određuje samo kako računalo za vođenje zbirki za obradu posebnih kategorija osobnih podataka[113] i središnje računalo sustava mora, između ostalog, biti opremljeno mehanizmom zaštite od računalnih virusa i drugih štetnih programa.[114] Uredba se ne odnosi na druge vrste osobnih podataka, osim onih koji su određeni kao posebne kategorije, ali primjereni stupanj zaštite i za ostale osobne podatke[115] može se zahtijevati temeljem odredbi ZZOP-a koje zahtijevaju informiranost ispitanika o davanju podataka na korištenje drugim osobama.[116] No to je nemoguće provesti ukoliko su podaci uslijed njihove nezaštićenosti dostupni svima s određenim tehničkim predznanjem, a pored toga ZZOP propisuje pravo ispitanika na naknadu štete ukoliko su podaci neovlašteno dani na korištenje drugoj osobi.[117] Temeljem općih načela odgovornosti za štetu, voditelja zbirke osobnih podataka trebalo bi smatrati odgovornim ukoliko nije primijenio adekvatan sustav zaštite podataka.

6.4. Odgovornost proizvođača računalnih programa

Računalni programi su proizvodi koje tvrtke proizvođači prodaju na tržištu. Postavlja se pitanje može li proizvođač računalnog programa, odnosno autor, biti odgovoran za to što svojim programom nije spriječio neovlašteno pristupanje tom programu, podacima pohranjenim u tom programu ili drugim programima na tom računalu. Nije od tolike važnosti nezaštićenost programskog koda manjih programa, već se pitanje postavlja za programe koji čine operativni sustav računala ili računalne mreže. Nesporna bi bila odgovornost prodavatelja ukoliko stvar ima materijalni nedostatak u slučaju kada je, primjerice, oštećen jedan ili dio nosača programa, pa zbog toga dođe do neadekvatne instalacije, ali ostali isti proizvodi rade ispravno.

Rasprave se vode oko odgovornosti za sigurnosne postavke operativnog sustava, i to napose sustava Microsoft Windows. Upravo su računala koja koriste ovaj operativni sustav bila česta meta raznih ilegalnih napada. Činjenica da je ovaj sustav meta napada, ne mora značiti da je

[111] Narodne novine, br.103/03., 118/06., nadalje: ZZOP, čl. 8. st. 4.

[112] Narodne novine, br.139/04.

[113] Članak 8. st. 1. ZZOP-a određuje koji se osobni podaci smatraju posebnom kategorijom osobnih podataka, a to su podaci koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku.

[114] Čl. 7. t. 3. Uredbe.

[115] Kao što su primjerice brojevi kreditnih kartica, polja interesa zanimljiva za marketinške agencije isl.

[116] Čl. 9. st. 2. ZZOP-a.

[117] Čl. 26. st. 2. ZZOP-a.

najnesigurniji, već je najrašireniji među korisnicima kojima računarstvo nije primarna struka, računalo im je samo sredstvo za rad, pa stoga i nemaju visoki stupanj stručnog obrazovanja za rad s računalom.[118] Iako sudovi u Sjedinjenim Američkim Državama (gdje je sjedište većine značajnijih proizvođača računalnih programa i s najdužom praksom korištenja računala te imaju i najrazvijenije stavove u sudskoj praksi) nisu zauzeli stajalište kako je proizvođač računalnog programa objektivno odgovoran za proizvod koji prodaje ukoliko je morao znati da ne zadovoljava sigurnosne kriterije prilikom stavljanja u promet, postoje argumentacije za i protiv uvođenja takve odgovornosti. Ukoliko bi sudovi zauzeli takav stav, autori programa morali bi ga puno duže testirati, ali bi ipak imali odgovorniji stav prema svom proizvodu kojeg puštaju u promet. To bi rezultiralo višom cijenom programa budući da bi u nju bilo uračunato više radnih sati, ali i veći rizik od plaćanja naknada štete kupcima.[119] Time se isto otvara pitanje koje je rizike mogao autor programa predvidjeti, budući da se ilegalna aktivnost razvija barem jednakom brzinom kao i tehnološki napredak, pa je nešto što je bilo u trenutku izrade i testiranja programa teško zamislivo, postalo moguće, a uz pad cijena računalne opreme i dostupno sve širem krugu osoba.

Daljnje pitanje koje se pojavljuje u praksi jest odgovornost proizvođača programa nakon što se određeni rizik pojavio, te je on izradio "zakrpu" za svoj program, ali korisnik o tome nije informiran i nije ju preuzeo i na taj način osigurao podatke na svom računalu. U tom slučaju isključiva je odgovornost korisnika koji je dužan brinuti se o svom računalu.[120] Kao što je ranije izloženo, rok u kojem korisnik mora preuzeti dodatke programu koji koristi nije definiran, već se može govoriti o razumnom roku, koji se mjeri prema iskustvima konkurenata.[121] U slučaju *Cyber Promotions v. Apex* radilo se o osobi čija je profesionalna djelatnost vezana za pružanje usluga informacijskog društva, ali se postavlja pitanje koji se standardi mogu zahtijevati od osoba kojima je računalo samo priručno sredstvo u radu, kao primjerice liječnicima ili odvjetnicima, koji u okviru obavljanja svoje djelatnosti moraju prikupljati posebne kategorije osobnih podataka svojih

[118] Vidi hipotetski primjer liječnika koji koristi računalo opisan u članku: Cammarata, M.: Chi paga i danni provocati dai virus?, Interlex, 6.12.2001.<www.interlex.it>, gdje se ukazuje na nedostatke programa za čitanje elektroničke pošte koji u svojim inicijalnim postavkama ima uključenu opciju automatskog otvaranja dodataka elektroničkoj pošti, bez potrebe korisnika pokrenuti otvaranje dodatka. Takva je postavka privlačna upravo za početnike koji još ne vladaju svim potrebnim znanjima, a takve osobe pogotovo nemaju znanje mijenjanja tih naprednih opcija, niti su upućene u rizike koje one donose. Uzet je primjer liječnika jer oni upravo gotovo isključivo u obavljanju svoje profesije prikupljaju posebnu kategoriju osobnih podataka svojih pacijenata.

[119] Vidi: Pinkney, K.R., op. cit., str. 71.-73. i tamo citirana djela.

[120] *Ibid.* str. 74.

[121] Vidi odluku: State of Maine, Public Utilities Commission, Docket No. 2000-894, 30. travnja 2003., <http://www.maine.gov/mpuc/orders/2000/2000-849o.htm>.

klijenata, ali prema dosadašnjim uvjetima za obavljanje svoje djelatnosti nisu obvezni imati informatičko obrazovanje.

Hrvatski Zakon o obveznim odnosima predviđa izvanugovornu odgovornost proizvođača za neispravan proizvod, kojom je predviđena objektivna odgovornost, ali je mala mogućnost ostvarivanja te odgovornosti za računalne programe koji nisu pouzdani. Naime, iako računalni programi jesu proizvodi, ZOO zahtijeva kumulativno ispunjenje pretpostavki za odgovornost, a to je da se proizvod koristi isključivo za osobnu uporabu i da šteta na oštećenikovoj stvari izvan proizvoda prelazi kunsku protuvrijednost od 500 eura, budući da pravo na naknadu postoji samo za dio štete koji prelazi taj iznos.[122] Isto tako je potrebno uzeti u obzir i druga ograničenja odgovornosti koja postavlja Zakon, a to je da se proizvod ne smatra neispravnim samo zbog toga što je naknadno bolji proizvod stavljen u promet,[123] te da stanje znanosti ili tehničkog znanja u vrijeme stavljanja proizvoda u promet nije omogućavalo otkrivanje neispravnosti.[124]

Umanjenje sigurnosti računala dovodi i do zaraza drugim štetnim programima, kao i u slučaju kada je SONY BMG pokušala zaštiti svoje legitimno pravo i spriječiti neovlašteno kopiranje glazbenih compact – diskova, ugradivši određeni program koji se sam instalirao kada je comapct disc stavljen u računalo. Svrha programa bila je mogućnost nadzora nad umnožavanjem i kopiranjem glazbe, ali je, kako bi mogao neprimjetno o tome izvješćivati SONY BMG, smanjivao sigurnosnu razinu zaštite računala i na taj način omogućavao drugim štetnim programima koji se nalaze na internetu instalaciju na tom računalu.[125] Nagodbom je utvrđeno kako programi koji su dodani glazbi na nosaču zvuka i služe za zaštitu autorskih prava čine računala na kojima se sluša glazba "ranjivima" prema štetnim programima koje šire treći, uključujući viruse, trojanske konje i *spyware*.[126] Taj program bio je dodan glazbi i sve njegove funkcije nisu bile u cijelosti ili pravovaljano predstavljene prilikom prodaje nosača zvuka kao proizvoda.[127] Naknada je po svakom oštećeniku relativno mala, budući da su im ponuđeni ili simbolični iznos ili preuzimanje drugih glazbenih

[122] ZOO, čl. 1073. st. 2. i 3. Iako zakon predviđa i naknadu štete imovinske izazvanu smrću ili tjelesnom ozljedom, teško je zamisliva situacija kada bi računalo koje se koristi samo za osobnu uporabu moglo uslijed neadekvatnih sigurnosnih postavki izazvati smrt ili tjelesnu povredu. To je moguće kod računala koja upravljaju drugim strojevima, ali tada to nije osobna uporaba računalnog programa.

[123] ZOO, čl. 1075. st. 2.

[124] ZOO, čl. 1078., st. 1., al. 5.

[125] Vidi sudsku nagodbu koju je sklopila SONY BMG s učincima class actiona-a (učinak prema svim oštećenicima, a ne samo onima koji su pokrenuli postupak, ako se jave u određenom roku) s oštećenim kupcima njihovih CD-a. United States Disctrict Court for the Southern District of New York, In re SONY BMG CD Technologies Litigation, No 1:05-cv-09575 (NRB), 28. prosinca 2005. godine.

[126] *Ibid*. Vidi točku I. E nagodbe.

[127] *Ibid.* Vidi točku I. F nagodbe.

izdanja istog izdavača u MP3 formatu, a obvezani su i sanirati štetu na način da na svojim internetskim stranicama daju računalni program koji će vratiti prvotno sigurnosno stanje na oštećena računala.[128] Iako SONY BMG izrijekom utvrđenom u nagodbi izjavljuje kako potpis nagodbe nema značaj utvrđivanja postojanja odgovornosti i stupnja odgovornosti, a isto tako se utvrđuje da naknada nije utvrđena utvrđivanjem stvarne štete, budući da bi to zahtijevalo dugotrajni postupak koji bi morao uključiti i stručna vještačenja. Stoga se prilikom određivanja naknade u nagodbi vodilo onime što je utvrđeno za vrijeme dugotrajnih pregovora stranaka, vodeći računa o snazi argumenata i protuargumenata, te troškovima i rizicima vođenja parnice.[129]

I prema hrvatskom pravu prodavatelji ovih nosača zvuka snosili bi dio odgovornosti za proizvod kojem nisu deklarirali sve karakteristike prilikom prodaje, a koje su proizvođaču prilikom izrade programa bile poznate.[130] Kako bi se spriječio daljnji nastanak šteta i stvaranje nezaštićenih računala, u Sjedinjenim Američkim Državama, SONY BMG je obvezana objaviti tekst nagodbe s popisom nosača zvuka koji sadrže taj oblik zaštite u mnogim novinama namijenjenim različitim interesnim skupinama, kako bi svi mogli biti upoznati s tim podatkom i zatražiti verziju u MP3 formatu, a i taj nosač zvuka ne slušati putem računala, odnosno ako to čine, upoznati su s rizikom kojem se izlažu.[131]

Korisnici tih nosača zvuka u Republici Hrvatskoj nisu upoznati s tim rizicima, i neosnovano bi bilo očekivati od dobrog gospodarstvenika, a kamoli od dobrog domaćina, praćenje stranih magazina i / ili dnevnog tiska u kojima je objavljen popis nosača zvuka koji predstavljaju rizik za sigurnost informatičkog sustava. Stoga se kriteriji prema kojima je određena radnja krajnja nepažnja u Sjedinjenim Američkim Državama ne mogu primijeniti u Hrvatskoj i osoba koja je predvidjela određene postavke na svom računalu ne može biti odgovorna za štetu koja je nastala zbog neadekvatnog sustava zaštite, a koji nije uspostavljen voljom korisnika računala, već činjenicom da je u predmetno računalo stavljen nosač zvuka. Ovaj učinak usporediv

[128] *Ibid.* Vidi točku III. C. nagodbe.

[129] *Ibid.* Vidi točku XI. D. nagodbe

[130] ZOO, čl. 401. st. 1. t. 5. Ovakav nosač zvuka nema uobičajene karakteristike koje se od tog proizvoda očekuju, već ima i određene dodatne štetne učinke, o kojima prodavatelj nije izvijestio kupca. Slušanje glazbe na računalo na kojem se i radi nije neuobičajena aktivnost, a korisnik računala koji to čini ne smatra kako čini neku radnju kojom bi svoje računalo dovodio u stanje opasnosti od zaraze štetnim računalnim programima. Radnja slušanja glazbe ne može se usporediti s korištenjem računala koje je spojeno na internet, a koje nema program za zaštitu od virusa ili otvaranje privitka poruke od nepoznatog pošiljatelja koja sadrži ne previše smislen tekst ili potpuno neosoban tekst.

[131] Vidi točku VI. B. 5. nagodbe sa SONY BMG gdje se navode sve novine u kojima je podatke o nagodbi trebalo objaviti, a to su: *USA Today, People magazine, Rolling Stone, Spin magazin, Los Angeles Times, New York Daily News, New York Post, Chicago Tribune* i *Atlanta Journal – Constitution*.

je sa štetom koja nastaje od trojanskog konja, gdje korisnik nije znao koji program ugrađuje, ali ne u cijelosti. Kod trojanskog konja koji se krije u nekom drugom programu koji je skinut s interneta, prilikom instalacije propuštena je dužna pažnja koja zahtijeva prethodno testiranje računalnog programa na računalu koje ne sadrži bitne podatke, a tek potom instalaciju tog programa na računalo koje se koriti u radu. U slučaju nosača zvuka koji sadrži trojanskog konja odgovornost korisnika još je manja, budući da računalni program nije uobičajeni sastojak nosača zvuka.

7. Zaključak

Štetni računalni programi postaju sve raširenija pojava i otežavaju rad na računalu. Iako u svakodnevnom govoru koristimo izraz virus, zapravo se radi o različitim vrstama štetnih programa koji imaju svoje različite izvore i različite učinke, pa stoga i njihovi tvorci različito odgovaraju. Tvorci štetnih računalnih programa ukoliko ih čine namjerno, odgovorni su za štetu koja nastaje širenjem tih programa, isto kao i naručitelji tih programa, ali pravi je problem utvrditi tko su oni i gdje se nalaze. A i u slučaju kada se to utvrdi, oštećenici se rijetko pojavljuju sa zahtjevom za naknadu štete zbog toga što je ostvarenje naknade s obzirom na imovinu štetnika upitno, a trošak za dokazivanje nastale štete je relativno velik.

Pri nemogućnosti ispunjenja ugovorne obveze uslijed virusa postavlja se pitanje je li zaraza virusom nešto što je bilo predvidivo i što se moglo spriječiti ili, iako se moglo očekivati, nije se moglo poduzeti ništa kako bi se spriječilo. Možda bi se mogla povući analogija između zaštite od virusa u pogledu računala i zaštita građevina od potresa. Kao što postoje za određena područja na zemlji odredbe o tome koju jačinu potresa moraju moći izdržati građevine, tako bi i za određene djelatnosti morali postojati standardi koji stupanj zaštite moraju imati određena računala. I isto kao što se u izvanrednim okolnostima može dogoditi potres veće jačine od one na koju moraju biti otporne zgrade, tada ne postoji odgovornost graditelja za oštećenja nastala na zgradi budući da su nastala uslijed više sile. Isto tako, nisu svi računalni štetni programi isti, pa je za utvrđivanje odgovornosti potrebno konzultirati stručnjake, da li se i u kojoj mjeri šteta mogla spriječiti ili barem jesu li štetne posljedice mogle biti umanjene. Sličan stav je zapravo i zauzet u presudi *Cyber Promotions v. Apex Global Information Services*, kada je sud naglasio kako se tužitelj bavi slanjem tzv. "*spam*a", i kako je tuženik s time bio upoznat, te je morao primijeniti veće mjere sigurnosti, budući da se radi o djelatnosti koja u praksi češće biva žrtvom ilegalnih računalnih napada.

Sudska praksa Sjedinjenih Američkih Država postavila je vrlo visoke kriterije korisnicima računala u pogledu uspostave tehničke zaštite i tehničkog nadzora svojih računala. Pitanje je jesu li ti kriteriji primjereni

svim korisnicima, od davatelja usluga informacijskog društva, do svih drugih osoba koje se više ili manje u svom radu koriste računalima.

U našoj zemlji nema objavljene sudske prakse u pogledu odgovornosti za štetu nastalu zbog štetnih računalnih programa, što ne znači kako takve štete nema. Gospodarska praksa još uvijek nije definirala poslove informatičke službe i poslove korisnika, pa s toga ne može ni biti jasne podjele odgovornosti između korisnika i osobe koja za tog korisnika obavlja informatičku potporu. Kada se sagledaju moguće štetne posljedice štetnih programa, uviđa se kako zadiranjem računalne tehnologije u naše živote u svakom pogledu, sama šteta nije više vezana samo uz gubitak ili oštećenje podataka na računalu nego i za daleko vrednija dobra, od osobnih podataka koji mogu biti divulgirani ili pribavljeni putem virusa, do fizičkog integriteta osoba, kada, primjerice, računala upravljaju vratima u bolnicama ili raznim elektroničkim strojevima. Nedefiniranost obveza dovodi do upitnosti odgovornosti. Nesporno je u slučaju kada računalo upravlja strojem koji je po sebi opasna stvar. Tada računalo čini dio opasne stvari i tada postoji objektivna odgovornost vlasnika stroja prema trećima. Većina takvih strojeva ima inkorporirano računalo koje nema mogućnosti kontakta s računalnim mrežama, niti je moguće samom korisniku zadirati u programe koji su u tom računalu, pa tako niti neovlaštenim osobama, osim u slučaju direktnog fizičkog kontakta i namjernog modificiranja ugrađenih programa. Međutim, postoje i strojevi koji su vezani na računalo koje mora biti spojeno na računalnu mrežu kako bi se mogla jednostavno vršiti nadogradnja programa i proširivati funkcije samog stroja ili usavršavati postojećih funkcija. Tada postoji opasnost zaraze tog računala virusom i disfunkcije u radu stroja, koja može rezultirati štetom. U tim slučajevima iako postoji objektivna odgovornost vlasnika stroja prema trećima, radi postavljanja regresnog zahtjeva prema proizvođaču potrebno je utvrditi dužnosti korisnika u pogledu sigurnosne zaštite od virusa tog računala i sigurnosti samog programa. Ali i u slučajevima kada se računalo koristi samo za pohranu baza podataka i dokumenata, te kao zamjena za pisaći stroj, korisnik mora znati kako stroj koji koristi radi, te koje su moguće posljedice činjenja ili propuštanja određenih radnji. Brzi napredak tehnologije otežava te zadatke, stoga je potrebno predvidjeti u planu uvođenja novih tehnologija period upoznavanja s istima, kako bi rad na njima bio siguran. Svaka osoba koja radi za računalom mora biti svjesna svoje odgovornosti s obzirom na podatke kojima se koristi, ali i odgovornosti prema sebi i svom radu. Novi štetni programi nastaju svakoga dana i koristeći računalo koje stupa u interakciju s drugim računalima, moramo biti svjesni rizika koje to sa sobom nosi, te upoznavajući stroj koji koristimo u radu spoznati i svoja ograničenja i razmisliti koje posljedice može donijeti svaki naš klik mišem.

Summary

FORMS OF DAMAGE CAUSED BY COMPUTER VIRUSES AND LIABILITY FOR DAMAGE

In the introductory part of this article, the author describes forms of computer malware and damage they can cause. Subsequently, she presents cases of liability of the malware authors for damage their programs have caused, problems related to discovering the responsible person and establishing his responsibility, as well as the problems of establishing the actual amount of damage and obligations of injured persons directed toward reducing the damage or even preventing it completely. Moreover, viruses and similar malware may render impossible, or significantly harden, the fulfillment of obligations deriving from contract on providing IT services. The article therefore defines contracts related to companies providing IT services, lists rights and obligations of the parties to these contracts, and describes consequences that may occur if one of the parties gets infected by computer virus. The US case-law in such cases has been presented together with underpinning reasoning, that eventually influenced the European legislation in a way that it accepted principle of IT services provider's liability.

Key words: *liability for damage, damage, contract on IT services, contractual liability, tort, computer virus, malware.*

Zusammenfassung

SCHÄDEN DURCH COMPUTER-VIREN UND HAFTUNG DAFÜR

Die Autorin beschreibt in der Einleitung die Formen beschädigter Rechnerprogramme und die Folgen, die durch diese entstehen können. Danach legt sie Fälle von Haftung der Autoren schädlicher infizierter? Programme für die Schäden, die sie hervorgerufen haben und Probleme hinsichtlich der Entdeckung der verantwortlichen Person dar, sowie Probleme bei der Feststellung des entstandenen Schadens, sowie die Pflicht des Geschädigten den Schaden zu verringern und sein Entstehen überhaupt zu verhindern. Außerden können Viren und ihnen ähnliche schädliche Programme die Ausführung der Pflichten der Vertragsparteien aus dem Vertrag zur Dienstleistung von Informationsgesellschaften verhindern oder erschweren. In der Arbeit werden Verträge der Informationsgesellschaften definiert, wobei die Rechte und Pflichten der Vertragsparteien angeführt werden sowie die Folgen, die entstehen können, wenn eine der Parteien von einem Virus angefallen wird. Es werden Auffassungen der Gerichtspraxis in

den USA bei solchen Fällen dargelegt und die Gründe für die Entschuldigung solcher Auffasssungen, die auch in der europäischen Gesetzgebung zur Annahme des Prinzips der Haftung des Dienstleisters geführt haben.

Schlüsselwörter: *Haftung für Schaden, Schaden, Vertrag, Vertrag über die Dienstleistung von Informationsgesellschaften, Vertragshaftung, außervertragliche Haftung, Computer-Virus (malware).*

Sommario

FORME DI DANNO DA VIRUS INFORMATICI E RESPONSABILITÀ PER DANNO

Nella parte introduttiva del lavoro l'autrice descrive le forme dei danni informatici e le conseguenze dannose che essi possono causare. In seguito l'autrice presenta i casi di responsabilità per danno degli autori di programmi dannosi che i loro programmi hanno causato, i problemi relativi alla scoperta della persona responsabile e all'affermazione della sua responsabilità, così come i problemi nella definizione dell'ammontare effettivo del danno e delle obbligazioni delle persone danneggiate riguardo la riduzione o la completa prevenzione del danno. Inoltre i virus e altri simili programmi dannosi possono rendere impossibile o significativamente più difficile l'adempimento delle obbligazioni derivanti dal contratto di fornitura di servizi informatici. Nel lavoro si definiscono i contratti relativi alle società che forniscono servizi informatici, si elencano i diritti e le obbligazioni delle parti di questi contratti, e si descrivono le conseguenze che possono aversi se una delle parti viene infettata da virus informatico. Sono presentate le prassi giudiziali negli Stati Uniti d'America insieme con le argomentazioni utilizzate, che alla fine hanno influenzato la legislazione europea in modo che accogliesse il principio della responsabilità del fornitore di servizi informatici.

Parole chiave: *responsabilità per danno, danno, contratto di servizi informatici, responsabilità contrattuale, responsabilità extracontrattuale, virus informatico (malware).*